Identity and Access Management

API Reference

Issue 02

Date 2023-09-14

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

Contents

1 Before You Start

1.1 Overview

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

You can use IAM through the console or application programming interfaces (APIs). This document describes how to use APIs to perform operations on IAM, such as creating users and user groups and obtaining tokens. If you intend to access IAM through APIs, ensure that you are familiar with IAM concepts. For details, see **Service Overview**.

1.2 API Calling

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

1.3 Endpoints

An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions.

Table 1-1 lists IAM endpoints. IAM is a global service with all data stored in the Global service project. All APIs of IAM can be called using the endpoint of the

Global region. To facilitate access to region-specific services using APIs or the CLI, some APIs of IAM are also provided for specific regions. To call these APIs, use the endpoint of the region (see **Constraints**) closest to you.

Table 1-1 IAM endpoints

Region Name	Region ID	Endpoint
Global	global	iam.myhuaweicloud.com
CN North-Beijing1	cn-north-1	iam.cn-north-1.myhuaweicloud.com
CN North-Beijing2	cn-north-2	iam.cn-north-2.myhuaweicloud.com
CN North-Beijing4	cn-north-4	iam.cn-north-4.myhuaweicloud.com
CN East-Shanghai1	cn-east-3	iam.cn-east-3.myhuaweicloud.com
CN East-Shanghai2	cn-east-2	iam.cn-east-2.myhuaweicloud.com
CN South-Guangzhou	cn-south-1	iam.cn-south-1.myhuaweicloud.com
CN South-Shenzhen	cn-south-2	iam.cn-south-2.myhuaweicloud.com
CN Southwest-Guiyang1	cn-southwest-2	iam.cn-southwest-2.myhuaweicloud.com
CN-Hong Kong	ap-southeast-1	iam.ap-southeast-1.myhuaweicloud.com
AP-Bangkok	ap-southeast-2	iam.ap-southeast-2.myhuaweicloud.com
AP-Singapore	ap-southeast-3	iam.ap-southeast-3.myhuaweicloud.com
AP-Jakarta	ap-southeast-4	iam.ap-southeast-4.myhuaweicloud.com

Region Name	Region ID	Endpoint
AF-Johannesburg	af-south-1	iam.af-south-1.myhuaweicloud.com
LA-Santiago	la-south-2	iam.la-south-2.myhuaweicloud.com
EU-Dublin	eu-west-101	iam.myhuaweicloud.eu
EU-Paris	eu-west-0	iam.eu-west-0.myhuaweicloud.com
TR-Istanbul	tr-west-1	iam.tr-west-1.myhuaweicloud.com
ME-Abu Dhabi-OP5	ae-ad-1	iam.ae-ad-1.myhuaweicloud.com

1.4 Constraints

The number of IAM resources that you can create is determined by your quota. For details, see **Notes and Constraints**.

1.5 Parameters

The following table lists a few API parameters and their names displayed on the console.

Table 1-2 API parameters

API Parameter	Name Displayed on the Console	How to Obtain on the Console
domain	Account	**Obtaining Account, IAM User, and Project Information**
domain_id or tenant_id	Account ID	
domain_name	Account name	
user	IAM user	**Obtaining Account, IAM User, and Project Information**
user_id	IAM user ID	

API Parameter	Name Displayed on the Console	How to Obtain on the Console
user_name	IAM user name	
group	User group	Obtaining User Group Information
group_id	User group ID	
group_name	User group name	
project	Project	Obtaining Account, IAM User, and Project Information
project_id	Project ID	
project_name	Project name	
agency	Agency	Obtaining Agency Information
agency_id	Agency ID	
agency_name	Agency name	

1.6 Basic Concepts

Common concepts used when you call APIs are described as follows:

- Account

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

- User

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

  An IAM user can view the account ID and user ID on the **My Credentials** page of the console. The account name, username, and password will be required for API authentication.

- 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 Global region and specific regions. The Global region provides common cloud services for all tenants, and a specific region provides services of the same type or provides special services for specific tenants.

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

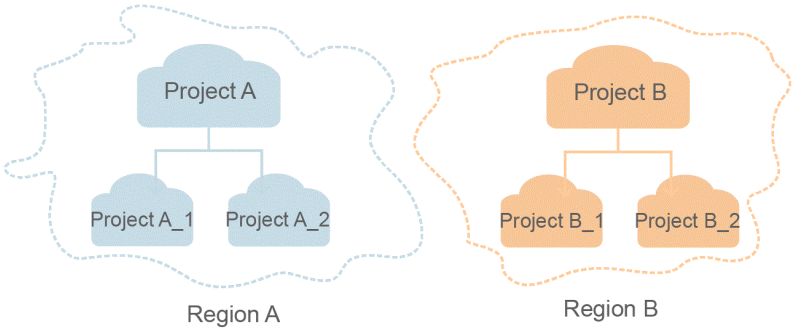
- AZ

  An Availability Zone (AZ) contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.

- Project

  Projects group and isolate resources (including compute, storage, and network resources) across physical regions. A default project is provided for each region, and subprojects can be created under each default project. Users can be granted permissions to access all resources in a specific project. If you need more refined access control, you can create subprojects under a default project and purchase resources in subprojects. Then you can assign required permissions for users to access only the resources in specific subprojects.

  Figure 1-1 Project isolating model

- Enterprise Project

  Enterprise projects group and manage resources across regions. Resources in enterprise projects are logically isolated from each other. An enterprise project can contain resources of multiple regions, and resources can be added to or removed from enterprise projects.

  For details about how to obtain enterprise project IDs and features, see the **Enterprise Management User Guide**.

2 API Overview

Token Management

API	Description
Obtaining a User Token Through Password Authentication	Obtain a user token through username/password-based authentication.
Obtaining a User Token Through Password and Virtual MFA Authentication	Obtain a user token using a username, password, and virtual MFA code on condition that virtual MFA–based login protection has been enabled.
Obtaining an Agency Token	Obtain an agency token.
Verifying a Token	Used by the administrator to verify the token of an IAM user or used by an IAM user to verify their own token.

Access Key Management

API	Description
Obtaining a Temporary Access Key and Security Token Through an Agency	Obtain a temporary access key and security token by using an agency.
Obtaining a Temporary Access Key and Security Token Through a Token	Obtain a temporary access key and security token using a token.

API	Description
Creating a Permanent Access Key	Used by the administrator to create a permanent access key for an IAM user or used by an IAM user to create a permanent access key.
Querying Permanent Access Keys	Used by the administrator to query all permanent access key of an IAM user or used by an IAM user to query all of their own permanent access keys.
Querying a Permanent Access Key	Used by the administrator to query the specified permanent access key of an IAM user or used by an IAM user to query one of their own permanent access keys.
Modifying a Permanent Access Key	Used by the administrator to modify the specified permanent access key of an IAM user or used by an IAM user to modify one of their own permanent access keys.
Deleting a Permanent Access Key	Used by the administrator to delete the specified permanent access key of an IAM user or used by an IAM user to delete one of their own permanent access keys.

Region Management

API	Description
Querying Regions	Query regions.
Querying Region Details	Query region details.

Project Management

API	Description
Querying Project Information	Query project information.
Listing Projects	Used by the administrator to list the projects accessible to a specified IAM user or used by an IAM user to list accessible projects.
Listing Projects Accessible to an IAM User	List the projects in which resources are accessible to a specified IAM user.
Creating a Project	Provided for the administrator to create a project.
Modifying Project Information	Provided for the administrator to modify project information.

API	Description
Querying Project Information	Query the detailed information about a project based on the project ID.
Changing Project Status	Provided for the administrator to change the status of a specified project. The project status can be normal or suspended.
Querying Project Information and Status	Provided for the administrator to query project details and status.
Querying the Quotas of a Project	Query the quotas of a specified project.

Account Management

API	Description
Querying Account Information Accessible to an IAM User	Query the account information that is accessible to a specified IAM user.
Querying the Password Strength Policy	Query the password strength policy, including the regular expression and description, of a specified account.
Querying the Regular Expression or Description of a Password Strength Policy	Query the password strength policy, including the regular expression and description, of a specified account based on specified conditions.
Querying the Quotas of an Account	Query the quotas of a specified account.

IAM User Management

API	Description
Listing IAM Users	Provided for the administrator to list all IAM users.
Querying IAM User Details (Recommended)	Used by the administrator to query the details about a specified IAM user or used by an IAM user to query their own details, including the mobile number and email address.

API	Description
Querying IAM User Details	Used by the administrator to query the details about a specified IAM user or used by an IAM user to query their own details, excluding the mobile number and email address.
Querying the User Groups to Which an IAM User Belongs	Used by the administrator to query the groups of a specified IAM user or used by an IAM user to query their own groups.
Querying the IAM Users in a Group	Used by the administrator to query the IAM users in a user group.
Creating an IAM User (Recommended)	Provided for the administrator to create an IAM user.
Creating an IAM User	This API is provided for the administrator to create an IAM user.
Changing the Login Password	Used by an IAM user to change the login password.
Modifying IAM User Information (Recommended)	Used by an IAM user to modify its basic information.
Modifying IAM User Information (Recommended)	Provided for the administrator to modify IAM user information.
Modifying User Information	Provided for the administrator to modify IAM user information.
Deleting an IAM User	Provided for the administrator to delete an IAM user.
Querying MFA Device Information of IAM Users	Provided for the administrator to query the MFA device information of IAM users.
Querying the MFA Device Information of an IAM User	Used by the administrator to query the MFA device information of a specified IAM user or used by an IAM user to query their own MFA device information.
Querying Login Protection Configurations of IAM Users	Provided for the administrator to query the login protection configurations of IAM users.
Querying the Login Protection Configuration of an IAM User	Used by the administrator to query the login protection configuration of a specified IAM user or used by an IAM user to query their own login protection configuration.

API	Description
Modifying the Login Protection Configuration of an IAM User	Provided for the administrator to modify the login protection configuration of an IAM user.
Binding a Virtual MFA Device	Bind a virtual MFA device to an IAM user.
Unbinding a Virtual MFA Device	Unbind the virtual MFA device bound to an IAM user.
Creating a Virtual MFA Device	Create a virtual MFA device for an IAM user.
Deleting a Virtual MFA Device	Provided for the administrator to delete the virtual MFA device created for an IAM user.

User Group Management

API	Description
Listing User Groups	Provided for the administrator to list all user groups.
Querying User Group Details	Provided for the administrator to query user group information.
Creating a User Group	Provided for the administrator to create a user group.
Updating User Group Information	Provided for the administrator to update user group information.
Deleting a User Group	Provided for the administrator to delete a user group.
Checking Whether an IAM User Belongs to a User Group	Provided for the administrator to check whether an IAM user belongs to a specified user group.
Adding an IAM User to a User Group	Provided for the administrator to add an IAM user to a specified user group.
Removing an IAM User from a User Group	Used by the administrator to remove an IAM user from a specified user group.

Permissions Management

API	Description
Listing Permissions	Provided for the administrator to list all permissions.
Querying Permission Details	Provided for the administrator to query permission details.
Querying Permissions of a User Group for a Global Service Project	Provided for the administrator to query the permissions of a user group for the global service project.
Querying Permissions of a User Group for a Region-specific Project	Provided for the administrator to query the permissions of a user group for a region-specific project.
Granting Permissions to a User Group for a Global Service Project	Provided for the administrator to grant permissions to a user group for the global service project.
Granting Permissions to a User Group for a Region-specific Project	Provided for the administrator to grant permissions to a user group for a region-specific project.
Checking Whether a User Group Has Specified Permissions for a Global Service Project	Provided for the administrator to check whether a user group has specified permissions for the global service project.
Checking Whether a User Group Has Specified Permissions for a Region-specific Project	Provided for the administrator to check whether a user group has specified permissions for a region-specific project.
Querying All Permissions of a User Group	Provided for the administrator to query all permissions that have been assigned to a user group.
Checking Whether a User Group Has Specified Permissions for All Projects	Provided for the administrator to check whether a user group has specified permissions for all projects.

API	Description
Removing Specified Permissions of a User Group in All Projects	Provided for the administrator to remove the specified permissions of a user group for all projects.
Removing Permissions of a User Group for a Global Service Project	Provided for the administrator to remove the specified permissions of a user group for the global service project.
Removing the Permissions of a User Group for a Region-specific Project	Provided for the administrator to remove the specified permissions of a user group for a region-specific project.
Granting Permissions to a User Group for All Projects	Provided for the administrator to grant permissions to a user group for all projects.

Custom Policy Management

API	Description
Listing Custom Policies	Provided for the administrator to list all custom policies.
Querying Custom Policy Details	Provided for the administrator to query the details of a specified custom policy.
Creating a Custom Policy for Cloud Services	Provided for the administrator to create a custom policy for cloud services.
Creating a Custom Policy for Agencies	Provided for the administrator to create a custom policy for agencies.
Modifying a Custom Policy for Cloud Services	Provided for the administrator to modify a custom policy for cloud services.
Modifying a Custom Policy for Agencies	Provided for the administrator to modify a custom policy for agencies.
Deleting a Custom Policy	Provided for the administrator to delete a custom policy.

Agency Management

API	Description
Listing Agencies	Provided for the administrator to list agencies that match specified conditions.
Querying Agency Details	Provided for the administrator to query the details about an agency.
Creating an Agency	Provided for the administrator to create an agency.
Modifying an Agency	Provided for the administrator to modify an agency.
Deleting an Agency	Provided for the administrator to delete an agency.
Querying Permissions of an Agency for a Global Service Project	Provided for the administrator to query the permissions of an agency for the global service project.
Querying Permissions of an Agency for a Region-specific Project	Provided for the administrator to query the permissions of an agency for a region-specific project.
Granting Permissions to an Agency for a Global Service Project	Provided for the administrator to grant permissions to an agency for the global service project.
Granting Permissions to an Agency for a Region-specific Project	Provided for the administrator to grant permissions to an agency for a region-specific project.
Checking Whether an Agency Has Specified Permissions for a Global Service Project	Provided for the administrator to check whether an agency has specified permissions for a global service project.
Checking Whether an Agency Has Specified Permissions for a Region-specific Project	Provided for the administrator to check whether an agency has specified permissions for a region-specific project.
Removing Permissions of an Agency for a Global Service Project	Provided for the administrator to remove the specified permissions of an agency for a global service project.
Removing Permissions of an Agency for a Region-specific Project	Provided for the administrator to remove the specified permissions of an agency for a region-specific project.

API	Description
Querying All Permissions of an Agency	Provided for the administrator to query all permissions that have been assigned to an agency.
Granting Specified Permissions to an Agency for All Projects	Provided for the administrator to grant specified permissions to an agency for all projects.
Checking Whether an Agency Has Specified Permissions	Provided for the administrator to check whether an agency has specified permissions.
Removing Specified Permissions of an Agency in All Projects	Provided for the administrator to remove the specified permissions of an agency in all projects.

Enterprise Project Management

API	Description
Querying User Groups Associated with an Enterprise Project	Query the user groups associated with the enterprise project of a specified ID.
Querying the Permissions of a User Group Associated with an Enterprise Project	Query the permissions of a user group associated with the enterprise project of a specified ID.
Granting Permissions to a User Group Associated with an Enterprise Project	Grant permissions to a user group associated with the enterprise project of a specified ID.
Removing Permissions of a User Group Associated with an Enterprise Project	Remove the permissions of a user group associated with an enterprise project.
Querying the Enterprise Projects Associated with a User Group	Query the enterprise projects associated with a user group.
Querying the Enterprise Projects Directly Associated with an IAM User	Query the enterprise projects associated with an IAM user.
Querying Users Directly Associated with an Enterprise Project	Query the users directly associated with a specified enterprise project.

API	Description
Querying Permissions of a User Directly Associated with an Enterprise Project	Query the permissions of a user directly associated with a specified enterprise project.
Granting a User Permissions for an Enterprise Project	Grant a user permissions for an enterprise project.
Removing Permissions of a User Directly Associated with an Enterprise Project	Remove the permissions of a user directly associated with a specified enterprise project.

Security Settings

API	Description
Modifying the Operation Protection Policy	Provided for the **administrator** to modify the operation protection policy.
Querying the Operation Protection Policy	Query the operation protection policy.
Modifying the Password Policy	Provided for the **administrator** to modify the password policy.
Querying the Password Policy of an Account	Query the password policy.
Modifying the Login Authentication Policy	Provided for the **administrator** to modify the login authentication policy.
Querying the Login Authentication Policy	Query the login authentication policy.
Modifying the ACL for Console Access	Provided for the **administrator** to modify the ACL for console access.
Querying the ACL for Console Access	Query the ACL for console access.
Modifying the ACL for API Access	Provided for the **administrator** to modify the ACL for API access.
Querying the ACL for API Access	Query the ACL for API access.

Federated Identity Authentication Management

API	Description
SP Initiated	Obtain a federated authentication token using the OpenStack Client or ShibbolethECP Client.
IdP Initiated	Obtain a federated authentication token in the IdP-initiated mode. The **Client4ShibbolethIdP** script is used as an example.
Listing Identity Providers	List all identity providers.
Querying Identity Provider Details	Query the details about an identity provider.
Creating an Identity Provider	Provided for the **administrator** to register an identity provider.
Modifying a SAML Identity Provider	Provided for the **administrator** to update an identity provider.
Deleting a SAML Identity Provider	Provided for the **administrator** to delete an identity provider.
Listing Mappings	List all mappings.
Querying Mapping Details	Query the details of a mapping.
Registering a Mapping	Provided for the **administrator** to register a mapping.
Updating a Mapping	Provided for the **administrator** to update a mapping.
Deleting a Mapping	Provided for the **administrator** to delete a mapping.
Listing Protocols	List all protocols.
Querying Protocol Details	Query the details of a protocol.
Registering a Protocol	Provided for the **administrator** to register a protocol, that is, to associate a protocol with an identity provider.
Updating a Protocol	Provided for the **administrator** to update the protocol associated with a specified identity provider.
Deleting a Protocol	Provided for the **administrator** to delete the protocol associated with a specified identity provider.
Querying a Metadata File	Provided for the **administrator** to query the metadata file imported to IAM for an identity provider.

API	Description
Querying the Metadata File of Keystone	Query the metadata file of Keystone.
Importing a Metadata File	Provided for the administrator to import a metadata file.
Obtaining an Unscoped Token (IdP Initiated)	Obtain an unscoped token through IdP-initiated federated identity authentication.
Obtaining a Scoped Token	Obtain a scoped token through federated identity authentication.
Obtaining a Token with an OpenID Connect ID Token	Obtain a federated identity authentication token using an OpenID Connect ID token.
Obtaining an Unscoped Token with an OpenID Connect ID Token	Obtain an unscoped token using an OpenID Connect ID token.
Listing Accounts Accessible to Federated Users	List the accounts whose resources are accessible to federated users.

Custom Identity Brokers

API	Description
Obtaining a Login Token	Obtain a token for logging in through a custom identity broker.

Version Information Management

API	Description
Querying the Version Information of Keystone APIs	Query the version information of Keystone APIs.
Querying Information About Keystone API 3.0	Obtain the information about Keystone API 3.0.

Services and Endpoints

API	Description
Listing Services	List all services.
Querying Service Details	Query the details of a service.
Querying the Service Catalog	Query the service catalog corresponding to **X-Auth-Token** contained in the request.
Listing Endpoints	List all endpoints.
Querying Endpoint Details	Query the details of an endpoint.

3 Calling APIs

3.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for **obtaining a user token through password authentication** as an example to demonstrate how to call an API. The obtained token contains the user identity and permissions information and can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

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

Table 3-1 Parameter description

Parameter	Description
URI-scheme	Protocol used to transmit requests. All APIs use HTTPS.
Endpoint	Domain name or IP address of the server running the REST service. The endpoint varies between services in different regions. It can be obtained from **Before You Start**. For example, the endpoint of IAM in the **EU-Dublin** region is **iam.myhuaweicloud.eu**.
resource-path	Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.

Parameter	Description
query-string	Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "*Parameter name*=*Parameter value*". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain a token in the EU-Dublin region, obtain the endpoint of IAM (**iam.myhuaweicloud.eu**) for this region and the **resource-path** (**/v3/auth/tokens**) in the URI of the API for **obtaining a user token through password authentication**. Then, construct the URI as follows:

https://v3/auth/tokens

```
https://iam.myhuaweicloud.eu/v3/auth/tokens
```

NOTE

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

Request Methods

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

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

For example, in the API used for **obtaining a user token through password authentication**, the request method is POST and the request is as follows:

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens
```

Request Header

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

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**.
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to **obtain a user token through**

password authentication. This API is the only one that does not require authentication.

NOTE

In addition to supporting token-based authentication, public cloud APIs also support authentication using AK/SK. During AK/SK-based authentication, an SDK is used to sign the request, and the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) header fields are automatically added to the request. For more information, see **AK/SK-based Authentication**.

The API used to **obtain a user token through password authentication** does not require authentication. Therefore, only the **Content-Type** field needs to be added to requests for calling the API. An example of such requests is as follows:

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens
Content-Type: application/json
```

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.

In the case of the API used to obtain a user token (**Obtaining a User Token Through Password Authentication**), the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Replace *username*, *domainname*, ******** (login password), and *xxxxxxxxxxxxxxxxx* (project ID) with the actual values. To learn how to obtain a project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

NOTE

The **scope** parameter specifies where a token takes effect. The value can be **project** or **domain**. In the preceding example, the value of **scope** is **project**, indicating that the obtained token takes effect only for the resources in a specified project. If the value of **scope** is **domain**, the obtained token takes effect for all resources of the specified account. For details, see the API for **obtaining a user token through password authentication**.

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens
Content-Type: application/json

{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
```



```
        "project": {
            "id": "xxxxxxxxxxxxxxxxxx"
        }
    }
  }
}
```

If all data required for the API request is available, you can send the request to call the API through **curl**, **Postman**, or coding. In the response header for the API used to **obtain a user token through password authentication**, **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

3.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

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

Token-based Authentication

NOTE

The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API.

A token can be obtained by calling the API for **obtaining a user token through password authentication**. Calling an IAM API requires a global token, that is, to get a token by calling this API, set **auth.scope** to **domain** in the request body.

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "domain": {
            "name": "IAMDomain"
          },
          "name": "IAMUser",
          "password": "IAMPassword"
        }
      }
    },
    "scope": {
      "domain": {
        "name": "IAMDomain"
      }
    }
  }
}
```

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** can be added to a request as follows:

```
GET https://iam.myhuaweicloud.eu/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK-based Authentication

NOTE

AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.

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

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

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

Status Code

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

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

For example, if status code **201** is returned for calling the API **obtaining a user token through password authentication**, the request is successful.

Response Header

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

In the response header for the API used to **obtain a user token through password authentication**, **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

Figure 3-1 Header fields of the response to the request for obtaining a user token

Response Body

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

The following is part of the response body for the API used to **obtain a user token through password authentication**:

```
{
    "token": {
        "expires_at": "2019-02-13T06:52:13.855000Z",
        "methods": [
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "region_id": "eu-west-101",
.....
```

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

```
{
    "error_msg": "The format of message is error",
    "error_code": "AS.0001"
}
```

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

4 Getting Started

4.1 Periodic Rotation of Access Keys

Scenario

Enterprise users usually use access keys (AK/SKs) to access cloud resources through APIs. They are advised to make access keys automatically rotate to reduce potential security risks.

This section guides you through rotating access keys by calling APIs. You can also automate rotation of access keys using programmatic methods.

Prerequisites

Before performing operations on the access keys of another **IAM user** as an **administrator**, ensure that you have been assigned the **Security Administrator** role. If you will perform operations on your own access keys as an IAM user, you do not need any special permissions assigned.

General Procedure

The following steps are involved to periodically rotate your access keys:

1. Create an access key.
2. Query the time when all of your access keys or a specified access key is created, and determine whether they need to be rotated.
3. Delete the old access key.
4. Create a new access key.

The following APIs will be used in this example:

- **Creating a Permanent Access Key**
- **Listing Permanent Access Keys**
- **Querying a Permanent Access Key**
- **Deleting a Permanent Access Key**

Step 1: Create a Permanent Access Key

URI: POST /v3.0/OS-CREDENTIAL/credentials

For details about the API, see **Creating a Permanent Access Key**.

- Example Request

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials
```

```
{
   "credential": {
      "description": "IAMDescription",
      "user_id": "07609fb9358010e21f7bc003751..."
   }
}
```

- Example Response

```
{
   "credential": {
      "access": "P83EVBZJMXCYTMUII...",
      "create_time": "2020-01-08T06:25:19.014028Z",
      "user_id": "07609fb9358010e21f7bc003751...",
      "description": "IAMDescription",
      "secret": "TTqAHPbhWorg9ozx8Dv9MUyzYnOKDppxzHt...",
      "status": "active"

}
```

Step 2: Query the Creation Time of a Specified or All Access Keys

- Query the creation time of all access keys.

  URI: GET /v3.0/OS-CREDENTIAL/credentials

  For details about the API, see **Querying Permanent Access Keys**.

  - Example Request

    IAM user: Use the following API to query the creation time of all of your access keys.

    ```
    GET https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials
    ```

    Administrator: Use the following API to query the creation time of all access keys of another IAM user. (**076...** indicates the ID of the user to query.)

    ```
    GET https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials?user_id=076...
    ```

  - Example Response

    ```
    {
       "credentials": [
          {
             "access": "LOSZM4YRVLKOY9E8X...",
             "create_time": "2020-01-08T06:26:08.123059Z",
             "user_id": "07609fb9358010e21f7bc0037...",
             "description": "",
             "status": "active"
          },
          {
             "access": "P83EVBZJMXCYTMU...",
             "create_time": "2020-01-08T06:25:19.014028Z",
             "user_id": "07609fb9358010e21f7bc003751...",
    ```



```
            "description": "",
            "status": "active"
        }
    ]
}
```

- Query the creation time of a specified access key.

  URI: GET /v3.0/OS-CREDENTIAL/credentials/{access_key}

  For details about the API, see **Querying a Permanent Access Key**.

  – Example Request

  ```
  GET https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials/{access_key}
  ```

  – Example Response

  ```
  {
      "credential": {
          "last_use_time": "2020-01-08T06:26:08.123059Z",
          "access": "LOSZM4YRVLKOY9E8...",
          "create_time": "2020-01-08T06:26:08.123059Z",
          "user_id": "07609fb9358010e21f7bc00375....",
          "description": "",
          "status": "active"
      }
  }
  ```

Step 3: Delete the Old Access Key

URI: DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key}

For details about the API, see **Deleting a Permanent Access Key**.

- Example Request

  ```
  DELETE https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials/{access_key}
  ```

- Example Response

  This API does not have a response body. If the status code **204** is displayed, the access key is deleted successfully.

Step 4: Create a New Access Key

Repeat **Step 1: Create a Permanent Access Key**.

4.2 Federated Authentication for Enterprise Accounts

Scenario

Enterprises with multiple accounts in the public cloud can access the resources under these accounts through their own IdP system. To achieve this purpose, they can call APIs to configure federated identity authentication.

This section describes how to implement automatic federated authentication by calling APIs.

Prerequisites

Only **administrators** can perform the registration and import operations described in this section. Ensure that you have been assigned the **Security Administrator** role.

General Procedure

Perform the following steps to configure federated identity authentication for multiple accounts on the cloud:

1. Register an identity provider.
2. Register a mapping.
3. Register a protocol.
4. Import a metadata file.
5. Log in as a federated user.

The following APIs will be used in this example:

- **Registering an Identity Provider**
- **Registering a Mapping**
- **Registering a Protocol**
- **Importing a Metadata File**

Step 1: Register an Identity Provider

URI: PUT /v3/OS-FEDERATION/identity_providers/{id}

For details about the API, see **Creating an Identity Provider**.

- Example Request
  PUT https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{id}

```
{
    "identity_provider":{
        "description":"Stores ACME identities.",
        "enabled":true
    }
}
```

- Example Response

```
{
    "identity_provider": {
        "remote_ids": [],
        "enabled": true,
        "id": "ACME",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME",
            "protocols": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME/
protocols"
        },
        "description": "Stores ACME identities."
    }
}
```

Step 2: Register a Mapping

URI: PUT /v3/OS-FEDERATION/mappings/{id}

For details about the API, see **Registering a Mapping**.

- Example Request
  PUT https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings/{id}

```
{
    "mapping":{
```



```
    "rules":[
        {
            "local":[
                {
                    "user":{
                        "name":"LocalUser"
                    }
                },
                {
                    "group":{
                        "name":"LocalGroup"
                    }
                }
            ],
            "remote":[
                {
                    "type":"UserName"
                },
                {
                    "not_any_of":[
                        "Contractor",
                        "Guest"
                    ],
                    "type":"orgPersonType"
                }
            ]
        }
    ]
  }
}
```

- Example Response

```
{
    "mapping":{
        "id":"ACME",
        "links":{
            "self":"https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings/ACME"
        },
        "rules":[
            {
                "local":[
                    {
                        "user":{
                            "name":"LocalUser"
                        }
                    },
                    {
                        "group":{
                            "name":"LocalGroup"
                        }
                    }
                ],
                "remote":[
                    {
                        "type":"UserName"
                    },
                    {
                        "not_any_of":[
                            "Contractor",
                            "Guest"
                        ],
                        "type":"orgPersonType"
                    }
                ]
            }
        ]
    }
}
```


Step 3: Register a Protocol

URI: PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}

For details about the API, see **Registering a Protocol**.

- Example Request

```
PUT https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}
```

```
{
    "protocol":{
        "mapping_id":"ACME"
    }
}
```

- Example Response

```
{
    "protocol":{
        "id":"saml",
        "links":{
            "identity_provider":"https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME",
            "self":"https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME/protocols/saml"
        },
        "mapping_id":"ACME"
    }
}
```

Step 4: Import a Metadata File

URI: POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata

For details about the API, see **Importing a Metadata File**.

- Example Request

```
POST https://iam.myhuaweicloud.eu/v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata
```

```
{
    "domain_id":"d78cbac186b744899480f25bd022....",
    "metadata":"$metadataContent",
    "xaccount_type":""
}
```

- Example Response

```
{
    "message":"Import metadata successful"
}
```

Step 5: Log In as a Federated User

Configure federated authentication. For details, see **Identity Providers**.

4.3 Security Auditing on Permissions of IAM Users

Scenario

Enterprise users usually need to periodically audit the permissions of IAM users created in the public cloud, ensuring that IAM users only have the permissions required to complete certain tasks. Generally, only account administrators and

auditors have administration permissions for the IAM service, and IAM users should not have these permissions. Periodic security audit can be automatically implemented through APIs.

This section describes how to perform security audit on the permissions of IAM users by calling APIs. You can also implement periodic security audit using programmatic methods.

Prerequisites

To audit IAM user permissions as an auditor, ensure that you have been assigned the IAM ReadOnlyAccess policy (recommended) or **Security Administrator** role.

General Procedure

To audit the permissions of IAM users, perform the following procedure:

1. List all the user groups.
2. Query the permissions of each user group for the global service project.
3. Query the permissions of each user group for region-specific projects.
4. Determine the permissions to be audited and query the IAM users in each user group that has been assigned these permissions.

The following APIs will be used in this example:

- **Listing User Groups**
- **Querying Permissions of a User Group for the Global Service Project**
- **Querying Permissions of a User Group for a Region-specific Project**
- **Querying the IAM Users in a Group**

Step 1: List All the User Groups

URI: GET /v3/groups

For details about the API, see **Listing User Groups**.

- Example Request
  ```
  GET https://iam.myhuaweicloud.eu/v3/groups
  ```
- Example Response
  ```
  {
      "groups":[
          {
              "create_time":1536293929624,
              "description":"IAMDescription",
              "domain_id":"d78cbac186b744899480f25bd022....",
              "id":"5b050baea9db472c88cbae67e8d6....",
              "links":{
                  "self":"https://iam.myhuaweicloud.eu/v3/groups/5b050baea9db472c88cbae67e8d6...."
              },
              "name":"IAMGroupA"
          },
          {
              "create_time":1578107542861,
              "description":"IAMDescription",
              "domain_id":"d78cbac186b744899480f25bd022....",
              "id":"07609e7eb200250a3f7dc003cb7a....",
              "links":{
                  "self":"https://iam.myhuaweicloud.eu/v3/groups/07609e7eb200250a3f7dc003cb7a...."
  ```



```
            },
            "name":"IAMGroupB"
        }
    ],
    "links":{
        "self":"https://iam.myhuaweicloud.eu/v3/groups"
    }
}
```


Step 2: Query Permissions of Each User Group for the Global Service Project

URI: GET /v3/domains/{domain_id}/groups/{group_id}/roles

For details about the API, see **Querying Permissions of a User Group for a Global Service Project**.

- Example Request


```
GET https://iam.myhuaweicloud.eu/v3/domains/{domain_id}/groups/{group_id}/roles
```


- Example Response


```
{
    "links":{
        "self":"https://iam.myhuaweicloud.eu/v3/domains/d78cbac186b744899480f25bd022f468/groups/
077d71374b8025173f61c003ea0a11ac/roles"
    },
    "roles":[
        {
            "catalog":"CDN",
            "description":"Allow Query Domains",
            "description_cn":"Description of the permission in Chinese",
            "display_name":"CDN Domain Viewer",
            "flag":"fine_grained",
            "id":"db4259cce0ce47c9903dfdc195eb....",
            "links":{
                "self":"https://iam.myhuaweicloud.eu/v3/roles/db4259cce0ce47c9903dfdc195eb...."
            },
            "name":"system_all_11",
            "policy":{
                "Statement":[
                    {
                        "Action":[
                            "cdn:configuration:queryDomains",
                            "cdn:configuration:queryOriginServerInfo",
                            "cdn:configuration:queryOriginConfInfo",
                            "cdn:configuration:queryHttpsConf",
                            "cdn:configuration:queryCacheRule",
                            "cdn:configuration:queryReferConf",
                            "cdn:configuration:queryChargeMode",
                            "cdn:configuration:queryCacheHistoryTask",
                            "cdn:configuration:queryIpAcl",
                            "cdn:configuration:queryResponseHeaderList"
                        ],
                        "Effect":"Allow"
                    }
                ],
                "Version":"1.1"
            },
            "type":"AX"
        }
    ]
}
```


Step 3: Query Permissions of Each User Group for Region-specific Projects

URI: GET /v3/projects/{project_id}/groups/{group_id}/roles

For details about the API, see **Querying Permissions of a User Group for a Region-specific Project**.

- Example Request
  GET https://iam.myhuaweicloud.eu/v3/projects/{project_id}/groups/{group_id}/roles
- Example Response

```
{
    "links":{
        "self":"https://iam.myhuaweicloud.eu/v3/projects/065a7c66da0010992ff7c0031e5a..../groups/
077d71374b8025173f61c003ea0a..../roles"
    },
    "roles":[
        {
            "catalog":"AOM",
            "description":"AOM read only",
            "description_cn":"Description of the permission in Chinese",
            "display_name":"AOM Viewer",
            "flag":"fine_grained",
            "id":"75cfe22af2b3498d82b655fbb39d....",
            "links":{
                "self":"https://iam.myhuaweicloud.eu/v3/roles/75cfe22af2b3498d82b655fbb39d...."
            },
            "name":"system_all_30",
            "policy":{
                "Statement":[
                    {
                        "Action":[
                            "aom:*:list",
                            "aom:*:get",
                            "apm:*:list",
                            "apm:*:get"
                        ],
                        "Effect":"Allow"
                    }
                ],
                "Version":"1.1"
            },
            "type":"XA"
        }
    ]
}
```

Step 4: Determine the Permissions to Be Audited and Query IAM Users Granted These Permissions

URI: GET /v3/groups/{group_id}/users

For details about the API, see **Querying the IAM Users in a Group**.

- Example Request
  GET https://iam.myhuaweicloud.eu/v3/groups/{group_id}/users
- Example Response

```
{
    "links":{
        "self":"https://iam.myhuaweicloud.eu/v3/groups/07609e7eb200250a3f7dc003cb7a..../users"
    },
    "users":[
        {
            "description":"--",
            "domain_id":"d78cbac186b744899480f25bd022....",
            "enabled":true,
            "id":"07609fb9358010e21f7bc003751c....",
            "last_project_id":"065a7c66da0010992ff7c0031e5a....",
            "links":{
                "self":"https://iam.myhuaweicloud.eu/v3/users/07609fb9358010e21f7bc003751c...."
            },
```

```
            "name":"IAMUserA",
            "pwd_status":true
        },
        {
            "description":"",
            "domain_id":"d78cbac186b744899480f25bd022....",
            "enabled":true,
            "id":"076837351e80251c1f0fc003afe4....",
            "last_project_id":"065a7c66da0010992ff7c0031e5a....",
            "links":{
                "self":"https://iam.myhuaweicloud.eu/v3/users/076837351e80251c1f0fc003afe4...."
            },
            "name":"IAMUserB",
            "pwd_status":true
        }
    ]
}
```

5 API

5.1 Token Management

5.1.1 Obtaining a User Token Through Password Authentication

Function

This API is used to obtain a user token using the username and password. A token is an access credential issued to an IAM user to bear its identity and permissions.

When calling the APIs of IAM or other cloud services, you can use this API to obtain a user token for authentication.

The API can be called using both the global endpoint and region-specific endpoints.

Quick links

Obtaining a token as an IAM user

Obtaining a token using a master account

Obtaining a token using a HUAWEI ID

Obtaining a token using a Huawei Cloud account

Obtaining a token as a third-party system user

Validity period of a token

FAQs about obtaining a token

Related operations

- Obtaining a token as an IAM user

  See **Request Parameters**.
- Obtaining a token using a master account

  If **HUAWEI ID Information** is displayed on the **Basic Information** page of My Account, you are logged in with a HUAWEI ID. Otherwise, you are logged in with a Huawei Cloud account.
- Obtaining a token using a HUAWEI ID

  You cannot directly use a HUAWEI ID to obtain a token. You need to **create an IAM user**, **assign permissions to the user**, and use the user to obtain a token.
- Obtaining a token using a Huawei Cloud account

  See **Request Parameters**.
- Obtaining a token as a third-party system user

  If you are a user of a third-party system, you cannot obtain a token by using the username and password that you use for federated identity authentication. Instead, you should go to the Huawei Cloud login page, click **Forgot password**, click **Reset Huawei Cloud account password**, and set a password.
- Validity period of a token
  - The validity period of a token is 24 hours. Cache the token to prevent frequent API calling. Ensure that the token is valid while you use it. Using a token that will soon expire may cause API calling failures. Obtaining a new token does not affect the validity of the existing token.
  - The token will become invalid within 30 minutes if any of the following occurs:
    - The IAM user is deleted or disabled.
    - The IAM user's password or access key is changed.

        - The IAM user's permissions are changed (due to outstanding payments, OBT application approval, or permission modification).
    - If **The token must be updated** is returned when a token is used to call a cloud service API, the token has expired. You need to obtain a new token.
- FAQs about obtaining a token

  Incorrect user name or password: Check whether the entered user name and password are correct. If the username and password are correct but the error persists, **check whether you have used a HUAWEI ID to obtain a token**. A HUAWEI ID cannot be directly used to obtain a token. You need to create an IAM user, grant permissions to the user, and use the user to obtain a token.

  No API access permissions: Before calling an API, ensure that you have **enabled programmatic access**.
- Related operations
    - If login protection has been enabled and the verification method has been set to virtual MFA device, obtain a token as an IAM user by following the instructions provided in **Obtaining a User Token Through Password and Virtual MFA Authentication**.
    - To obtain a token with **Security Administrator** permissions, see **How Do I Obtain a Token with Security Administrator Permissions?**
    - For details on how to obtain a token using Postman, see **How Do I Obtain a User Token Using Postman?**

URI

POST /v3/auth/tokens

Table 5-1 Query parameters

Parameter	Mandatory	Type	Description
nocatalog	No	String	If this parameter is set, no catalog information will be displayed in the response. Any character string set for this parameter indicates that no catalog information will be displayed.

Request Parameters

Table 5-2 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

Table 5-3 Parameters in the request body

Parameter	Mandatory	Type	Description
auth	Yes	Object	Authentication information.

Table 5-4 auth

Parameter	Mandatory	Type	Description
identity	Yes	Object	Authentication parameters.
scope	No	Object	Application scope of the token. The value can be **project** or **domain**. **NOTE** • **If the scope is set to domain, the token applies to global services. If the scope is set to project, the token applies to project-level services.** • **If the scope is set to both project and domain, the project is used and you get a token for project-level services.** • **If the scope is left blank, you get a token for global services. You are advised to specify this parameter.**

Table 5-5 auth.identity

Parameter	Mandatory	Type	Description
methods	Yes	Array of strings	Authentication method. The content of this field is **["password"]**.

Parameter	Mandatory	Type	Description
password	Yes	Object	Password authentication information of an IAM user. **NOTE** • View your username and account name on the **My Credentials** page. For details, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. • This API uses a lockout mechanism to prevent brute force cracking. The account will be locked out if the number of unsuccessful login attempts reaches the maximum limit set by the **administrator**. For details, see **Account Lockout**.

Table 5-6 auth.identity.password

Parameter	Mandatory	Type	Description
user	Yes	Object	Information about the IAM user who is requesting to obtain a token.

Table 5-7 auth.identity.password.user

Parameter	Mandatory	Type	Description
domain	Yes	Object	Information about the account used to create the IAM user. For details about the relationship between accounts and IAM users, see **Relationship Between an Account and Its IAM Users**.
name	Yes	String	IAM user name.

Parameter	Mandatory	Type	Description
password	Yes	String	Password of the IAM user. **NOTE** • To obtain a token successfully, ensure that the password you provide is correct. • If your Huawei Cloud account has been upgraded to a HUAWEI ID, you cannot obtain a token using the HUAWEI ID. Instead, you can create an IAM user, grant the user required permissions, and obtain a token as the user. • If you are a user of a third-party system, you cannot obtain a token by using the username and password that you use for federated identity authentication. Go to the Huawei Cloud login page, click **Forgot password**, click **Reset Huawei Cloud account password**, and set a new password.

Table 5-8 auth.identity.password.user.domain

Parameter	Mandatory	Type	Description
name	Yes	String	Account name. For details about how to obtain the account name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Table 5-9 auth.scope

Parameter	Mandatory	Type	Description
domain	No	Object	If this field is set to **domain**, the token can be used to access global services, such as OBS. Global services are not subject to any projects or regions. For details about the service scope, see **System Permissions**. You can specify either **id** or **name**. **domain_id** is recommended.

Parameter	Mandatory	Type	Description
project	No	Object	If this field is set to **project**, the token can be used to access only services in specific projects, such as ECS. For details about the service scope, see **System Permissions**. You can specify either **id** or **name**.

Table 5-10 auth.scope.domain

Parameter	Mandatory	Type	Description
id	No	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. If **auth.scope** is set to **domain**, the obtained token can be used for global services. Either **id** or **name** must be specified.
name	No	String	Account name. For details about how to obtain the account name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. If **auth.scope** is set to **domain**, the obtained token can be used for global services. Either **id** or **name** must be specified.

Table 5-11 auth.scope.project

Parameter	Mandatory	Type	Description
id	No	String	Project ID. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. If **auth.scope** is set to **project**, the obtained token can be used for project-level services. Either **id** or **name** must be specified. The project ID varies depending on the region where the service is located.
name	No	String	Project name. For details about how to obtain the project name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. If **auth.scope** is set to **project**, the obtained token can be used for project-level services. Either **id** or **name** must be specified.

Example Request

- Request for obtaining a token for IAM user **IAMUser** (password: **IAMPassword**; account name: **IAMDomain**; scope: project **eu-west-101**) without displaying catalog information in the response You can obtain the IAM username and account name on the **My Credential** page of the console. For details, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens?nocatalog=true
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "domain": {
                        "name": "IAMDomain"        // Name of the account to which the IAM user belongs.
                    },
                    "name": "IAMUser",             // IAM user name.
                    "password": "IAMPassword"      // IAM user password.
                }
            }
        },
        "scope": {
            "project": {
                "name": "eu-west-101"              //Project name
            }
        }
    }
}
```

- Request for obtaining a token for IAM user **IAMUser** (password: **IAMPassword**; account name: **IAMDomain**; scope: **domain**) You can obtain the IAM username and account name on the **My Credential** page of the console. For details, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "domain": {
                        "name": "IAMDomain"        // Name of the account to which the IAM user belongs.
                    },
                    "name": "IAMUser",             // IAM user name.
                    "password": "IAMPassword"      // IAM user password.
                }
            }
        },
        "scope": {
            "domain": {
                "name": "IAMDomain"        // Name of the account to which the IAM user belongs.
            }
        }
    }
}
```

Response Parameters

Table 5-12 Parameters in the response header

Parameter	Type	Description
X-Subject-Token	String	Signed token, which is less than 32 KB.

Table 5-13 Parameters in the response body

Parameter	Type	Description
Token	Object	Token information.

Table 5-14 Token

Parameter	Type	Description
catalog	Array of objects	Catalog information.

Parameter	Type	Description
domain	Object	Account information of the IAM user who requests for the token. This parameter is returned only when the **scope** parameter in the request body has been set to **domain**.
expires_at	String	Time when the token will expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
issued_at	String	Time when the token was issued. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
methods	Array of strings	Method for obtaining the token.
project	Object	Project information of the IAM user. This parameter is returned only when the **scope** parameter in the request body has been set to **project**.
roles	Array of objects	Permissions information of the token.
user	Object	Information about the IAM user who requests for the token.

Table 5-15 Token.catalog

Parameter	Type	Description
endpoints	Array of objects	Endpoint information.
id	String	Service ID.
name	String	Service name.
type	String	Type of the service to which the API belongs.

Table 5-16 Token.catalog.endpoints

Parameter	Type	Description
id	String	Endpoint ID.

Parameter	Type	Description
interface	String	Visibility of the API. **public** indicates that the API is available for public access.
region	String	Region to which the endpoint belongs.
region_id	String	Region ID.
url	String	Endpoint URL.

Table 5-17 Token.domain

Parameter	Type	Description
name	String	Account name.
id	String	Account ID.

Table 5-18 Token.project

Parameter	Type	Description
domain	Object	Account information of the project.
id	String	Project ID.
name	String	Project name.

Table 5-19 Token.project.domain

Parameter	Type	Description
id	String	Account ID.
name	String	Account name.

Table 5-20 Token.roles

Parameter	Type	Description
name	String	Permission name.
id	String	Permission ID. The default value is **0**, which does not correspond to any permission.

Table 5-21 Token.user

Parameter	Type	Description
name	String	IAM user name.
id	String	IAM user ID.
password_expires_at	String	Password expiration time. If this parameter is not specified, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
domain	Object	Information about the account used to create the IAM user.

Table 5-22 Token.user.domain

Parameter	Type	Description
name	String	Name of the account used to create the IAM user.
id	String	Account ID.

Example Response

Status code: 201

The request is successful.

- Response to the request for obtaining a token for IAM user **IAMUser** (password: **IAMPassword**; account name: **IAMDomain**; scope: project **eu-west-101**) without displaying catalog information in the response

Parameters in the response header (obtained token)
X-Subject-Token:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...
Parameters in the response body

```
{
    "token": {
        "catalog": [],
        "expires_at": "2020-01-04T09:05:22.701000Z",
        "issued_at": "2020-01-03T09:05:22.701000Z",
        "methods": [
            "password"
        ],
        "project": {
            "domain": {
                "id": "d78cbac186b744899480f25bd022f...",
                "name": "IAMDomain"
            },
            "id": "aa2d97d7e62c4b7da3ffdfc11551f...",
            "name": "eu-west-101"
        },
        "roles": [
            {
```

```
            "id": "0",
            "name": "te_admin"
         },
         {
            "id": "0",
            "name": "op_gated_OBS_file_protocol"
         },
         {
            "id": "0",
            "name": "op_gated_Video_Campus"
         }
      ],
      "user": {
         "domain": {
            "id": "d78cbac186b744899480f25bd022f...",
            "name": "IAMDomain"
         },
         "id": "7116d09f88fa41908676fdd4b039e...",
         "name": "IAMUser",
         "password_expires_at": ""
      }
   }
}
```

- Response to the request for obtaining a token for IAM user **IAMUser** (password: **IAMPassword**; account name: **IAMDomain**; scope: **domain**)

  Parameters in the response header (obtained token)

  X-Subject-Token:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...

  Parameters in the response body

```
{
   "token": {
      "catalog": [
         {
            "endpoints": [
               {
                  "id": "33e1cbdd86d34e89a63cf8ad16a5f...",
                  "interface": "public",
                  "region": "*",
                  "region_id": "*",
                  "url": "https://iam.myhuaweicloud.eu/v3.0"
               }
            ],
            "id": "100a6a3477f1495286579b819d399...",
            "name": "iam",
            "type": "iam"
         },
         {
            "endpoints": [
               {
                  "id": "29319cf2052d4e94bcf438b55d143...",
                  "interface": "public",
                  "region": "*",
                  "region_id": "*",
                  "url": "https://bss.sample.domain.com/v1.0"
               }
            ],
            "id": "c6db69fabbd549908adcb861c7e47...",
            "name": "bssv1",
            "type": "bssv1"
         }
      ],
      "domain": {
         "id": "d78cbac186b744899480f25bd022f...",
         "name": "IAMDomain"
      },
      "expires_at": "2020-01-04T09:08:49.965000Z",
      "issued_at": "2020-01-03T09:08:49.965000Z",
      "methods": [
         "password"
      ],
```

```
        "roles": [
            {
                "id": "0",
                "name": "te_admin"
            },
            {
                "id": "0",
                "name": "secu_admin"
            },
            {
                "id": "0",
                "name": "te_agency"
            }
        ],
        "user": {
            "domain": {
                "id": "d78cbac186b744899480f25bd022f...",
                "name": "IAMDomain"
            },
            "id": "7116d09f88fa41908676fdd4b039e...",
            "name": "IAMUser",
            "password_expires_at": ""
        }
    }
}
```

Status code: 400

Invalid parameters. Check whether the request body complies with the JSON syntax.

```
{
    "error": {
        "code": 400,
        "message": "The request body is invalid",
        "title": "Bad Request"
    }
}
```

Status code: 401

Authentication failed.

- If you are a user of a third-party system, you cannot obtain a token by using the username and password that you use for federated identity authentication. Go to the Huawei Cloud login page, click **Forgot password**, click **Reset Huawei Cloud account password**, and set a new password.
- If your Huawei Cloud account has been upgraded to a HUAWEI ID, you cannot obtain a token using the HUAWEI ID. Instead, you can create an IAM user, grant the user required permissions, and obtain a token as the user.

```
{
    "error": {
        "code": 401,
        "message": "The username or password is wrong.",
        "title": "Unauthorized"
    }
}
```

Status Codes

Status Code	Description
201	The request is successful.

Status Code	Description
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.1.2 Obtaining a User Token Through Password and Virtual MFA Authentication

Function

This API is provided for IAM users to obtain a token through **username/password and virtual MFA authentication**. To use this API, ensure that **virtual MFA-based login protection has been enabled** for the IAM user. A token is an access credential issued to a user to bear its identity and permissions. When calling the APIs of IAM or other cloud services, you can use this API to obtain a token for authentication.

The API can be called using both the global endpoint and region-specific endpoints.

Quick links

Obtaining a token as an IAM user

Obtaining a token using a master account

Obtaining a token using a HUAWEI ID

Obtaining a token using a Huawei Cloud account

Obtaining a token as a third-party system user

Validity period of a token

FAQs about obtaining a token

Related operations

- Obtaining a token as an IAM user
  See **Request Parameters**.
- Obtaining a token using an account

If **HUAWEI ID Information** is displayed on the **Basic Information** page of My Account, you are logged in with a HUAWEI ID. Otherwise, you are logged in with a Huawei Cloud account.

- Obtaining a token using a HUAWEI ID

  You cannot directly use a HUAWEI ID to obtain a token. You need to **create an IAM user**, **assign permissions to the user**, and use the user to obtain a token.

- Obtaining a token using a Huawei Cloud account

  See **Request Parameters**.

- Obtaining a token as a third-party system user

  If you are a user of a third-party system, you cannot obtain a token by using the username and password that you use for federated identity authentication. Instead, you should go to the Huawei Cloud login page, click **Forgot password**, click **Reset Huawei Cloud account password**, and set a password.

- Validity period of a token
  - The validity period of a token is **24 hours**. Cache the token to prevent frequent API calling. Ensure that the token is valid while you use it. Using a token that will soon expire may cause API calling failures. Obtaining a new token does not affect the validity of the existing token.
  - The token will become invalid within 30 minutes if any of the following occurs:
    - The IAM user is deleted or disabled.
    - The IAM user's password or access key is changed.
    - The IAM user's permissions are changed (due to outstanding payments, OBT application approval, or permission modification).
  - If **The token must be updated** is returned when a token is used to call a cloud service API, the token has expired. You need to obtain a new token.

- FAQs about obtaining a token

  Incorrect user name or password: Check whether the entered user name and password are correct. If the username and password are correct but the error persists, **check whether you have used a HUAWEI ID to obtain a token**. A HUAWEI ID cannot be directly used to obtain a token. You need to create an IAM user, grant permissions to the user, and use the user to obtain a token.

  No API access permissions: Before calling an API, ensure that you have **enabled programmatic access**.

- Related operations
  - To obtain a token with **Security Administrator** permissions, see **How Do I Obtain a Token with Security Administrator Permissions?**
  - For details on how to obtain a token using Postman, see **How Do I Obtain a User Token Using Postman?**

URI

POST /v3/auth/tokens

Table 5-23 Query parameters

Parameter	Mandatory	Type	Description
nocatalog	No	String	If this parameter is set, no catalog information will be displayed in the response. Any character string set for this parameter indicates that no catalog information will be displayed.

Request Parameters

Table 5-24 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

Table 5-25 Parameters in the request body

Parameter	Mandatory	Type	Description
auth	Yes	Object	Authentication information.

Table 5-26 auth

Parameter	Mandatory	Type	Description
identity	Yes	Object	Authentication parameters.

Parameter	Mandatory	Type	Description
scope	Yes	Object	Application scope of the token. The value can be **project** or **domain**. **NOTE** • **If the scope is set to domain, the token applies to global services. If the scope is set to project, the token applies to project-level services.** • **If the scope is set to both project and domain, the project is used and you get a token for project-level services.** • **If the scope is left blank, you get a token for global services. You are advised to specify this parameter.**

Table 5-27 auth.identity

Parameter	Mandatory	Type	Description
methods	Yes	Array of strings	Authentication method. Options: • password • totp
password	Yes	Object	IAM user password authentication information. **NOTE** • View your username and account name on the **My Credentials** page. For details, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. • This API uses a lockout mechanism to prevent brute force cracking. The account will be locked out if the number of unsuccessful login attempts reaches the maximum limit set by the **administrator**. For details, see **Account Lockout**.
totp	Yes	Object	Authentication information. This parameter is mandatory only when virtual MFA–based login authentication is enabled.

Table 5-28 auth.identity.password

Parameter	Mandatory	Type	Description
user	Yes	Object	Information about the IAM user who is requesting to obtain a token.

Table 5-29 auth.identity.password.user

Parameter	Mandatory	Type	Description
domain	Yes	Object	Information about the account used to create the IAM user. For details about the relationship between accounts and IAM users, see **Relationship Between an Account and Its IAM Users**.
name	Yes	String	IAM user name.
password	Yes	String	Password of the IAM user. **NOTE** • To obtain a token successfully, ensure that the password you provide is correct. • If you are a user of a third-party system, you cannot obtain a token by using the username and password that you use for federated identity authentication. Go to the Huawei Cloud login page, click **Forgot password**, click **Reset Huawei Cloud account password**, and set a new password.

Table 5-30 auth.identity.password.user.domain

Parameter	Mandatory	Type	Description
name	Yes	String	Account name. For details about how to obtain the account name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Table 5-31 auth.identity.totp

Parameter	Mandatory	Type	Description
user	Yes	Object	IAM user information. Ensure that virtual MFA-based login protection has been enabled for the IAM user. For details, see **Critical Operations**.

Table 5-32 auth.identity.totp.user

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the IAM user for whom virtual MFA-based login protection has been enabled.
passcode	Yes	String	MFA verification code, which can be obtained from the virtual MFA device bound to the IAM user. For details, see **How Do I Obtain MFA Verification Codes?** **NOTE** To obtain a token successfully, ensure that the verification code you provide is correct.

Table 5-33 auth.scope

Parameter	Mandatory	Type	Description
domain	No	Object	If this field is set to **domain**, the token can be used to access global services, such as OBS. Global services are not subject to any projects or regions. For details about the service scope, see **System Permissions**. You can specify either **id** or **name**. **domain.id** is recommended.
project	No	Object	If this field is set to **project**, the token can be used to access only services in specific projects, such as ECS. For details about the service scope, see **System Permissions**. You can specify either **id** or **name**.

Table 5-34 auth.scope.domain

Parameter	Mandatory	Type	Description
id	No	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
name	No	String	Account name. For details about how to obtain the account name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Table 5-35 auth.scope.project

Parameter	Mandatory	Type	Description
id	No	String	Project ID. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
name	No	String	Project name. For details about how to obtain the project name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Example Request

- Example 1: Request for obtaining a token for IAM user **IAMUser** (password: **IAMPassword**; account name: **IAMDomain**; scope: **domain**) You can obtain the IAM username and account name on the **My Credential** page of the console. For details, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens
{
    "auth": {
        "identity": {
            "methods": [
                "password",
                "totp"
            ],
            "password": {
                "user": {
```

```
                "name": "IAMUser",                      // IAM user name.
                "password": "IAMPassword",              // IAM user password.
                "domain": {
                   "name": "IAMDomain"                  // Name of the account to which the IAM user
belongs.
                }
             }
          },
          "totp": {
             "user": {
                "id": "7116d09f88fa41908676fdd4b039e...",  // IAM user ID.
                "passcode": "******"                    // Virtual MFA verification code.
             }
          }
       },
       "scope": {
          "domain": {
             "name": "IAMDomain"                        // Name of the account to which the IAM
user belongs.
          }
       }
    }
}
```

- Example 2: Request for obtaining a token for IAM user **IAMUser** (password: **IAMPassword**; account name: **IAMDomain**; scope: project **eu-west-101**) without displaying catalog information in the response You can obtain the IAM username and account name on the **My Credential** page of the console. For details, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens?nocatalog=true
{
    "auth": {
       "identity": {
          "methods": [
             "password",
             "totp"
          ],
          "password": {
             "user": {
                "name": "IAMUser",                      // IAM user name.
                "password": "IAMPassword",              // IAM user password.
                "domain": {
                   "name": "IAMDomain"                  // Name of the account to which the IAM user
belongs.
                }
             }
          },
          "totp": {
             "user": {
                "id": "7116d09f88fa41908676fdd4b039e...",  // IAM user ID.
                "passcode": "******"                    // Virtual MFA verification code.
             }
          }
       },
       "scope": {
          "project": {
             "name": "eu-west-101"                      //Project name
          }
       }
    }
}
```


Response Parameters

Table 5-36 Parameters in the response header

Parameter	Type	Description
X-Subject-Token	String	Signed token.

Table 5-37 Parameters in the response body

Parameter	Type	Description
token	Object	Token information.

Table 5-38 token

Parameter	Type	Description
catalog	Array of objects	Catalog information.
domain	Object	Account information of the IAM user who requests for the token. This parameter is returned only when the **scope** parameter in the request body has been set to **domain**.
expires_at	String	Time when the token will expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
mfa_authn_at	String	MFA authentication time. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
issued_at	String	Time when the token was issued. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
methods	Array of strings	Method for obtaining the token.

Parameter	Type	Description
project	Object	Project information of the IAM user. This parameter is returned only when the **scope** parameter in the request body has been set to **project**.
roles	Array of objects	Permissions information of the token.
user	Object	Information about the IAM user who requests for the token.

Table 5-39 token.catalog

Parameter	Type	Description
endpoints	Array of objects	Endpoint information.
id	String	Service ID.
name	String	Service name.
type	String	Type of the service to which the API belongs.

Table 5-40 token.catalog.endpoints

Parameter	Type	Description
id	String	Endpoint ID.
interface	String	Visibility of the API. **public** indicates that the API is available for public access.
region	String	Region to which the endpoint belongs.
region_id	String	Region ID.
url	String	Endpoint URL.

Table 5-41 token.domain

Parameter	Type	Description
name	String	Account name.
id	String	Account ID.

Table 5-42 token.project

Parameter	Type	Description
domain	Object	Account information of the project.
id	String	Project ID.
name	String	Project name.

Table 5-43 token.project.domain

Parameter	Type	Description
id	String	Account ID.
name	String	Account name.

Table 5-44 token.roles

Parameter	Type	Description
name	String	Permission name.
id	String	Permission ID. The default value is **0**, which does not correspond to any permission.

Table 5-45 token.user

Parameter	Type	Description
name	String	IAM user name.
id	String	IAM user ID.
password_expires_at	String	Password expiration time. If this parameter is not specified, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
domain	Object	Information about the account used to create the IAM user.

Table 5-46 token.user.domain

Parameter	Type	Description
name	String	Name of the account used to create the IAM user.
id	String	ID of the account to which the IAM user belongs.

Example Response

Status code: 201

The request is successful.

- Example 1: Response to the request for obtaining a token for IAM user **IAMUser** (password: **IAMPassword**; account name: **IAMDomain**; scope: **domain**)

Parameters in the response header (obtained token)
X-Subject-Token:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...
Parameters in the response body

```
{
    "token": {
        "expires_at": "2020-01-04T09:08:49.965000Z",
        "mfa_authn_at": "2020-01-03T09:08:49.965000Z",
        "methods": [
            "password",
            "totp"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "id": "33e1cbdd86d34e89a63cf8ad16a5f...",
                        "interface": "public",
                        "region": "*",
                        "region_id": "*",
                        "url": "https://iam.myhuaweicloud.eu/v3.0"
                    }
                ],
                "id": "100a6a3477f1495286579b819d399...",
                "name": "iam",
                "type": "iam"
            },
            {
                "endpoints": [
                    {
                        "id": "29319cf2052d4e94bcf438b55d143...",
                        "interface": "public",
                        "region": "*",
                        "region_id": "*",
                        "url": "https://bss.sample.domain.com/v1.0"
                    }
                ],
                "id": "c6db69fabbd549908adcb861c7e47...",
                "name": "bssv1",
                "type": "bssv1"
            }
        ],
        "domain": {
            "id": "d78cbac186b744899480f25bd022f...",
            "name": "IAMDomain"
        },
```



```
    "roles": [
      {
        "id": "0",
        "name": "te_admin"
      },
      {
        "id": "0",
        "name": "secu_admin"
      },
      {
        "id": "0",
        "name": "te_agency"
      }
    ],
    "issued_at": "2020-01-03T09:08:49.965000Z",
    "user": {
      "domain": {
        "id": "d78cbac186b744899480f25bd022f...",
        "name": "IAMDomain"
      },
      "id": "7116d09f88fa41908676fdd4b039e...",
      "name": "IAMUser",
      "password_expires_at": ""
    }
  }
}
```


- Example 2: Response to the request for obtaining a token for IAM user **IAMUser** (password: **IAMPassword**; account name: **IAMDomain**; scope: project **eu-west-101**) without displaying catalog information in the response

  Parameters in the response header (obtained token)

  X-Subject-Token:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...

  Parameters in the response body


```
{
  "token": {
    "expires_at": "2020-01-04T09:05:22.701000Z",
    "mfa_authn_at": "2020-01-03T09:05:22.701000Z",
    "methods": [
      "password",
      "totp"
    ],
    "catalog": [],
    "roles": [
      {
        "id": "0",
        "name": "te_admin"
      },
      {
        "id": "0",
        "name": "op_gated_OBS_file_protocol"
      },
      {
        "id": "0",
        "name": "op_gated_Video_Campus"
      }
    ],
    "project": {
      "domain": {
        "id": "d78cbac186b744899480f25bd022f...",
        "name": "IAMDomain"
      },
      "id": "aa2d97d7e62c4b7da3ffdfc11551f...",
      "name": "eu-west-101"
    },
    "issued_at": "2020-01-03T09:05:22.701000Z",
    "user": {
      "domain": {
        "id": "d78cbac186b744899480f25bd022f...",
        "name": "IAMDomain"
```

```
            },
            "id": "7116d09f88fa41908676fdd4b039e...",
            "name": "IAMUser",
            "password_expires_at": ""
        }
    }
}
```

Status code: 400

Invalid parameters.

```
{
    "error": {
        "code": 400,
        "message": "The request body is invalid",
        "title": "Bad Request"
    }
}
```

Status code: 401

Authentication failed.

- If you are a user of a third-party system, you cannot obtain a token by using the username and password that you use for federated identity authentication. Go to the Huawei Cloud login page, click **Forgot password**, click **Reset Huawei Cloud account password**, and set a new password.
- If your Huawei Cloud account has been upgraded to a HUAWEI ID, you cannot obtain a token using the HUAWEI ID. Instead, you can create an IAM user, grant the user required permissions, and obtain a token as the user.

```
{
    "error": {
        "code": 401,
        "message": "The username or password is wrong.",
        "title": "Unauthorized"
    }
}
```

Status Codes

Status Code	Description
201	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.1.3 Obtaining an Agency Token

Function

This API is used to obtain an agency token.

For example, after a trust relationship is established between A and B, A is the delegating party and B is the delegated party. Then B can use this API to obtain an agency token. The obtained agency token can only be used to manage the resources that account B is delegated to manage. If account B needs to manage their own resources, account B needs to obtain a user token. For details, see **Delegating Resource Access to Another Account**.

A token is an access credential issued to a user to bear its identity and permissions. When calling the APIs of IAM or other cloud services, you can use this API to obtain a token for authentication.

The API can be called using both the global endpoint and region-specific endpoints.

NOTE

- The validity period of a token is 24 hours. Cache the token to prevent frequent API calling.
- Ensure that the token is valid while you use it. Using a token that will soon expire may cause API calling failures.

URI

POST /v3/auth/tokens

Table 5-47 Query parameters

Parameter	Mandatory	Type	Description
nocatalog	No	String	If this parameter is set, no catalog information will be displayed in the response. Any character string set for this parameter indicates that no catalog information will be displayed.

Request Parameters

Table 5-48 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Token with Agent Operator permissions of an IAM user created by delegated party B.

Table 5-49 Parameters in the request body

Parameter	Mandatory	Type	Description
auth	Yes	Object	Authentication information.

Table 5-50 auth

Parameter	Mandatory	Type	Description
identity	Yes	Object	Authentication parameters.
scope	Yes	Object	Usage scope of the token. The value can be **project** or **domain**. **NOTE** • **If the scope is set to domain, the token applies to global services. If the scope is set to project, the token applies to project-level services.** • **If the scope is set to both project and domain, the project is used and you get a token for project-level services.** • **If the scope is left blank, you get a token for global services. You are advised to specify this parameter.**

Table 5-51 auth.identity

Parameter	Mandatory	Type	Description
methods	Yes	Array of strings	Method for obtaining the token. Set this parameter to **assume_role**.
assume_role	Yes	Object	Details about the delegating account and agency.

Table 5-52 auth.identity.assume_role

Parameter	Mandatory	Type	Description
domain_id	No	String	Account ID of delegating party A. Either **domain_id** or **domain_name** must be set. You are advised to specify **domain_id**. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_name	No	String	Account name of delegating party A. Either **domain_id** or **domain_name** must be set. You are advised to specify **domain_id**. You can view the account name of delegating party A in the agency list on the IAM console.
agency_name	Yes	String	Name of the agency created by delegating party A. For details about how to obtain the agency name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Table 5-53 auth.scope

Parameter	Mandatory	Type	Description
domain	No	Object	If this field is set to **domain**, the token can be used to access global services, such as OBS. Global services are not subject to any projects or regions. For details about the service scope, see **System Permissions**. You can specify either **id** or **name**. **domain_id** is recommended.
project	No	Object	If this field is set to **project**, the token can be used to access only services in specific projects, such as ECS. For details about the service scope, see **System Permissions**. You can specify either **id** or **name**.

Table 5-54 auth.scope.domain

Parameter	Mandatory	Type	Description
id	No	String	Account ID of delegating party A. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. You can specify either **id** or **name**.
name	No	String	Account name of delegating party A. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. You can specify either **id** or **name**.

Table 5-55 auth.scope.project

Parameter	Mandatory	Type	Description
id	No	String	Project ID of delegating party A. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. You can specify either **id** or **name**.
name	No	String	Project name of delegating party A. For details about how to obtain the project name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. You can specify either **id** or **name**.

Example Request

- Request for using a user token with Agent Operator permissions of IAM user **IAMUserB** of delegated party B (account name: **IAMDomainB**) to obtain another token to manage the resources of delegating party A (account name: **IAMDomainA**) in the **eu-west-101** project through agency **IAMAgency**, without displaying catalog information in the response

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens?nocatalog=true
{
    "auth": {
        "identity": {
            "methods": [
                "assume_role"
            ],
            "assume_role": {
                "domain_name": "IAMDomainA",              // Name of the account to which the delegating party IAM user A belongs
                "agency_name": "IAMAgency"                // Name of the agency created by IAM user A
            }
        },
        "scope": {
            "project": {
                "name": "eu-west-101"                     //Project name
            }
        }
    }
}
```

- Request for using a user token with Agent Operator permissions of IAM user **IAMUserB** of delegated party B (account name: **IAMDomainB**) to obtain another token to manage all resources of delegating party A (account name: **IAMDomainA**) through agency **IAMAgency**

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens
{
    "auth": {
        "identity": {
            "methods": [
                "assume_role"
            ],
            "assume_role": {
```

```
            "domain_name": "IAMDomainA",            // Name of the account to which the
delegating party IAM user A belongs
            "agency_name": "IAMAgency"              // Name of the agency created by IAM user A
         }
      },
      "scope": {
         "domain": {
            "name": "IAMDomainA"                    // Name of the account to which the delegating
party IAM user A belongs
         }
      }
   }
}
```

Response Parameters

Table 5-56 Parameters in the response header

Parameter	Type	Description
X-Subject-Token	String	Signed token.

Table 5-57 Parameters in the response body

Parameter	Type	Description
token	Object	Token information.

Table 5-58 token

Parameter	Type	Description
methods	Array of strings	Method for obtaining the token.
expires_at	String	Time when the token will expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.
issued_at	String	Time when the token was issued. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.
assumed_by	Object	Information about delegated party B.
catalog	Array of objects	Catalog information.

Parameter	Type	Description
domain	Object	Account information of delegating party A. This parameter is returned only when the **scope** parameter in the request body has been set to **domain**.
project	Object	Project information of delegating party A. This parameter is returned only when the **scope** parameter in the request body has been set to **project**.
roles	Array of objects	Permissions information of the token.
user	Object	Information about the agency created by delegating party A.

Table 5-59 token.assumed_by

Parameter	Type	Description
user	Object	Information about an IAM user of delegated party B.

Table 5-60 token.assumed_by.user

Parameter	Type	Description
name	String	IAM user name.
id	String	IAM user ID.
domain	Object	Account information of delegated party B.
password_expires_at	String	Password expiration time of the IAM user. If this parameter is not specified, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Table 5-61 token.assumed_by.user.domain

Parameter	Type	Description
name	String	Account name of delegated party B.

Parameter	Type	Description
id	String	Account ID of delegated party B.

Table 5-62 token.catalog

Parameter	Type	Description
endpoints	Array of objects	Endpoint information.
id	String	Service ID.
name	String	Service name.
type	String	Type of the service to which the API belongs.

Table 5-63 token.catalog.endpoints

Parameter	Type	Description
id	String	Endpoint ID.
interface	String	Visibility of the API. **public** indicates that the API is available for public access.
region	String	Region to which the endpoint belongs.
region_id	String	Region ID.
url	String	Endpoint URL.

Table 5-64 token.domain

Parameter	Type	Description
name	String	Account name of delegating party A.
id	String	Account ID of delegating party A.

Table 5-65 token.project

Parameter	Type	Description
name	String	Project name of delegating party A.
id	String	Project ID of delegating party A.
domain	Object	Account information of delegating party A.

Table 5-66 token.project.domain

Parameter	Type	Description
name	String	Account name of delegating party A.
id	String	Account ID of delegating party A.

Table 5-67 token.roles

Parameter	Type	Description
name	String	Permission name.
id	String	Permission ID. The default value is **0**, which does not correspond to any permission.

Table 5-68 token.user

Parameter	Type	Description
name	String	Account name or agency name of delegating party A.
id	String	Agency ID.
domain	Object	Account information of delegating party A.

Table 5-69 token.user.domain

Parameter	Type	Description
id	String	Account ID of delegating party A.
name	String	Account name of delegating party A.

Example Response

Status code: 201

The request is successful.

Example 1: Response to the request for using a user token with Agent Operator permissions of IAM user **IAMUserB** of delegated party B (account name: **IAMDomainB**) to obtain another token to manage all resources of delegating party A (account name: **IAMDomainA**) through agency **IAMAgency**

Example 2: Response to the request for using a user token with Agent Operator permissions of IAM user **IAMUserB** of delegated party B (account name: **IAMDomainB**) to obtain another token to manage the resources of delegating

party A (account name: **IAMDomainA**) in the **eu-west-101** project through agency **IAMAgency**, without displaying catalog information in the response

- Example 1

```
Parameters in the response header
X-Subject-Token:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...
Parameters in the response body
{
   "token": {
      "expires_at": "2020-01-05T05:05:17.429000Z",
      "methods": [
         "assume_role"
      ],
      "catalog": [
         {
            "endpoints": [
               {
                  "id": "33e1cbdd86d34e89a63cf8ad16a5f49f",
                  "interface": "public",
                  "region": "*",
                  "region_id": "*",
                  "url": "https://iam.myhuaweicloud.eu/v3.0"
               }
            ],
            "id": "100a6a3477f1495286579b819d399e36",
            "name": "iam",
            "type": "iam"
         }
      ],
      "domain": {
         "id": "d78cbac186b744899480f25bd022f468",
         "name": "IAMDomainA"
      },
      "roles": [
         {
            "id": "0",
            "name": "op_gated_eip_ipv6"
         },
         {
            "id": "0",
            "name": "op_gated_rds_mcs"
         }
      ],
      "issued_at": "2020-01-04T05:05:17.429000Z",
      "user": {
         "domain": {
            "id": "d78cbac186b744899480f25bd022f468",
            "name": "IAMDomainA"
         },
         "id": "0760a9e2a60026664f1fc0031f9f205e",
         "name": "IAMDomainA/IAMAgency"
      },
      "assumed_by": {
         "user": {
            "domain": {
               "id": "a2cd82a33fb043dc9304bf72a0f38f00",
               "name": "IAMDomainB"
            },
            "id": "0760a0bdee8026601f44c006524b17a9",
            "name": "IAMUserB",
            "password_expires_at": ""
         }
      }
   }
}
```

- Example 2

```
Parameters in the response header
X-Subject-Token:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...
```


Parameters in the response body

```
{
    "token": {
        "expires_at": "2020-01-05T06:49:28.094000Z",
        "methods": [
            "assume_role"
        ],
        "catalog": [],
        "roles": [
            {
                "id": "0",
                "name": "op_gated_eip_ipv6"
            },
            {
                "id": "0",
                "name": "op_gated_rds_mcs"
            }
        ],
        "project": {
            "domain": {
                "id": "d78cbac186b744899480f25bd022f468",
                "name": "IAMDomainA"
            },
            "id": "aa2d97d7e62c4b7da3ffdfc11551f878",
            "name": "eu-west-101"
        },
        "issued_at": "2020-01-04T06:49:28.094000Z",
        "user": {
            "domain": {
                "id": "d78cbac186b744899480f25bd022f468",
                "name": "IAMDomainA"
            },
            "id": "0760a9e2a60026664f1fc0031f9f205e",
            "name": "IAMDomainA/IAMAgency"
        },
        "assumed_by": {
            "user": {
                "domain": {
                    "id": "a2cd82a33fb043dc9304bf72a0f38f00",
                    "name": "IAMDomainB"
                },
                "id": "0760a0bdee8026601f44c006524b17a9",
                "name": "IAMUserB",
                "password_expires_at": ""
            }
        }
    }
}
```

Status code: 400

Invalid parameters.

```
{
    "error": {
        "code": 400,
        "message": "The request body is invalid",
        "title": "Bad Request"
    }
}
```

Status code: 401

Authentication failed.

```
{
    "error": {
        "code": 401,
        "message": "The X-Auth-Token is invalid!",
        "title": "Unauthorized"
```



```
    }
}
```

Status code: 403

Access denied.

- The user token specified in **X-Auth-Token** for user B of delegated party B does not have the Agent Operator permission. Please apply for the required permission.

```
{
    "error": {
        "code": 403,
        "message": "You have no right to do this action",
        "title": "Forbidden"
    }
}
```

Status Codes

Status Code	Description
201	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied. (The possible cause of this error is that the delegated party does not have the Agent Operator permission.)
404	The requested resource cannot be found.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.1.4 Verifying a Token

Function

This API can be used by the **administrator** to verify the token of an IAM user or used by an IAM user to verify their own token. The administrator can only verify the token of an IAM user created using the account. If the token is valid, the detailed information about the token is returned.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/auth/tokens

Table 5-70 Query parameters

Parameter	Mandatory	Type	Description
nocatalog	No	String	If this parameter is set, no catalog information will be displayed in the response. Any character string set for this parameter indicates that no catalog information will be displayed.

Request Parameters

Table 5-71 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	A token with **Security Administrator** permissions is required if the **administrator** is requesting to verify the token of an IAM user. The user token (no special permission requirements) of an IAM user is required if the user is requesting to verify their own token.
X-Subject-Token	Yes	String	Token to be verified.

Example Request

Request for verifying a token

```
GET https://iam.myhuaweicloud.eu/v3/auth/tokens
```

Response Parameters

Table 5-72 Parameters in the response header

Parameter	Type	Description
X-Subject-Token	String	Verified token.

Table 5-73 Parameters in the response body

Parameter	Type	Description
token	Object	Token information.

Table 5-74 token

Parameter	Type	Description
catalog	Array of objects	Catalog information.
domain	Object	Account information of the IAM user whose token is to be verified. This parameter is returned only when the **scope** parameter in the request body has been set to **domain**.
expires_at	String	Time when the token will expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
issued_at	String	Time when the token was issued. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
methods	Array of strings	Method for obtaining the token.
project	Object	Project information of the IAM user. This parameter is returned only when the **scope** parameter in the request body has been set to **project**.
roles	Array of objects	Permissions information of the token.
user	Object	Information about the IAM user who requests for the token.

Table 5-75 token.catalog

Parameter	Type	Description
endpoints	Array of objects	Endpoint information.

Parameter	Type	Description
id	String	Service ID.
name	String	Service name.
type	String	Type of the service to which the API belongs.

Table 5-76 token.catalog.endpoints

Parameter	Type	Description
id	String	Endpoint ID.
interface	String	Visibility of the API. **public** indicates that the API is available for public access.
region	String	Region to which the endpoint belongs.
region_id	String	Region ID.
url	String	Endpoint URL.

Table 5-77 token.domain

Parameter	Type	Description
name	String	Account name.
id	String	Account ID.

Table 5-78 token.project

Parameter	Type	Description
domain	Object	Account information of the project.
id	String	Project ID.
name	String	Project name.

Table 5-79 token.project.domain

Parameter	Type	Description
id	String	Account ID.
name	String	Account name.

Table 5-80 token.roles

Parameter	Type	Description
name	String	Permission name.
id	String	Permission ID. The default value is **0**, which does not correspond to any permission.

Table 5-81 token.user

Parameter	Type	Description
name	String	IAM user name.
id	String	IAM user ID.
password_expires_at	String	Password expiration time. If this parameter is not specified, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
domain	Object	Information about the account used to create the IAM user.

Table 5-82 token.user.domain

Parameter	Type	Description
name	String	Name of the account used to create the IAM user.
id	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Example Response

Status code: 200

The request is successful.

```
Parameters in the response header
X-Subject-Token:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...
Parameters in the response body
{
    "token": {
        "expires_at": "2020-01-04T09:08:49.965000Z",
        "methods": [
```

```
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "id": "33e1cbdd86d34e89a63cf8ad16a5f49f",
                        "interface": "public",
                        "region": "*",
                        "region_id": "*",
                        "url": "https://iam.myhuaweicloud.eu/v3.0"
                    }
                ],
                "id": "100a6a3477f1495286579b819d399e36",
                "name": "iam",
                "type": "iam"
            },
            {
                "endpoints": [
                    {
                        "id": "29319cf2052d4e94bcf438b55d143832",
                        "interface": "public",
                        "region": "*",
                        "region_id": "*",
                        "url": "https://bss.sample.domain.com/v1.0"
                    }
                ],
                "id": "c6db69fabbd549908adcb861c7e47ca4",
                "name": "bssv1",
                "type": "bssv1"
            }
        ],
        "domain": {
            "id": "d78cbac186b744899480f25bd022f468",
            "name": "IAMDomain"
        },
        "roles": [
            {
                "id": "0",
                "name": "te_admin"
            },
            {
                "id": "0",
                "name": "secu_admin"
            },
            {
                "id": "0",
                "name": "te_agency"
            }
        ],
        "issued_at": "2020-01-03T09:08:49.965000Z",
        "user": {
            "domain": {
                "id": "d78cbac186b744899480f25bd022f468",
                "name": "IAMDomain"
            },
            "id": "7116d09f88fa41908676fdd4b039e95b",
            "name": "IAMUser",
            "password_expires_at": ""
        }
    }
}
```


Status code: 404

The requested resource cannot be found.


```
{
    "error": {
        "code": 404,
```

```
    "message": "X-Subject-Token is invalid in the request",
    "title": "Not Found"
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.2 Access Key Management

5.2.1 Obtaining a Temporary Access Key and Security Token Through an Agency

Function

This API is used to obtain a temporary access key and security token by using an agency.

Temporary access keys and security tokens are issued by the system to IAM users, and can be valid for 15 minutes to 24 hours. The temporary access key and security token follow the principle of least privilege. A temporary access key must be used together with a security token, and the **x-security-token** field must be included in the request header. For details, see **How Do I Use a Temporary AK/SK to Sign Requests?**

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3.0/OS-CREDENTIAL/securitytokens

Request Parameters

Table 5-83 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Token with Agent Operator permissions.

Table 5-84 Parameters in the request body

Parameter	Mandatory	Type	Description
auth	Yes	Object	Authentication information.

Table 5-85 auth

Parameter	Mandatory	Type	Description
identity	Yes	Object	Authentication parameters.

Table 5-86 auth.identity

Parameter	Mandatory	Type	Description
methods	Yes	Array of strings	Authentication method. Set this parameter to **["assume_role"]**.
assume_role	Yes	Object	Details about the delegating account and agency.

Parameter	Mandatory	Type	Description
policy	No	Object	Permissions to be assigned to the temporary access key and security token (currently the policy only applies to OBS). The final permissions of the temporary access key and security token are all the permissions assigned to the specified agency and defined in this parameter. For details about the format and syntax of IAM policies, see **Policies**.

Table 5-87 auth.identity.assume_role

Parameter	Mandatory	Type	Description
agency_name	Yes	String	Agency name. For details about how to obtain the agency name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_id	No	String	Account ID of the delegating party. Either **domain_id** or **domain_name** must be set. You are advised to specify **domain_id**.
domain_name	No	String	Account name of the delegating party. Either **domain_id** or **domain_name** must be set. You are advised to specify **domain_id**.
duration_seconds	No	Integer	Validity period (in seconds) of the AK/SK and security token. The value ranges from 15 minutes to 24 hours. The default value is 15 minutes.
session_user	No	Object	Enterprise user information of the delegating party.

Table 5-88 auth.identity.assume_role.session_user

Parameter	Mandatory	Type	Description
name	No	String	Enterprise user name of the delegating party. The name must consist of 1 to 32 characters, containing only letters (case-sensitive), digits, spaces, hyphens (-), underscores (_), and periods (.) and must start with a digit.

Table 5-89 auth.identity.policy

Parameter	Mandatory	Type	Description
Version	Yes	String	Policy version. When creating a custom policy, set this parameter to **1.1**. **NOTE** **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Yes	Array of objects	Statement of the policy. A policy can contain a maximum of eight statements.

Table 5-90 auth.identity.policy.Statement

Parameter	Mandatory	Type	Description
Action	Yes	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations.
Effect	Yes	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Condition	No	Map<String,Map<String,Array<String>>>	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**.
			NOTE
			Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**).
			`"Condition": {`
			`"StringEquals": {`
			`"obs:prefix": [`
			`"public"`
			`]`
			`}`
			`}`

Parameter	Mandatory	Type	Description
Resource	No	Array of strings	Cloud resource. **NOTE** • Format: *Service name*:*Region*:*Account ID*:*Resource type*:*Resource path*. Wildcard characters (*) are supported. For example, **obs:*:*:bucket:*** means all OBS buckets. • The region segment can be * or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists.

Response Parameters

Table 5-91 Parameters in the response body

Parameter	Type	Description
credential	Object	Authentication result.

Table 5-92 credential

Parameter	Type	Description
expires_at	String	Expiration time of the access key and security token. The response is UTC time.
access	String	AK.
secret	String	SK.
securitytoken	String	Obtained access key in ciphertext.

Example Request

- Request with **session_user** specified (containing the enterprise user name of the delegating party)

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/securitytokens
{
    "auth": {
        "identity": {
            "methods": [
                "assume_role"
            ],
            "assume_role": {
                "domain_name": "IAMDomainA",
                "agency_name": "IAMAgency",
```

```
            "duration_seconds": 3600,
            "session_user": {
                "name": "SessionUserName"
            }
        }
    }
  }
}
```

- Request with **policy** set to control the permissions assigned to the obtained temporary access key and security token (currently the policy applies only to OBS). The final permissions of the temporary access key and security token are the intersection of permissions assigned to the specified agency and defined in **policy**.

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/securitytokens
{
   "auth": {
      "identity": {
         "methods": [
            "assume_role"
         ],
         "policy": {
                  "Version": "1.1",
           "Statement": [{
          "Effect": "allow",
          "Action": [
                     "obs:object:*"
                    ],
          "Resource": ["obs:*:*:object:*"],
          "Condition": {
             "StringEquals": {
             "obs:prefix": ["public"]
             }
          }
       }]
           },
         "assume_role": {
            "domain_name": "IAMDomainA",
            "agency_name": "IAMAgency",
            "duration_seconds": 3600

         }
      }
   }
}
```

- Request without **session_user** and **policy** specified

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/securitytokens
{
   "auth": {
      "identity": {
         "methods": [
            "assume_role"
         ],
         "assume_role": {
            "domain_name": "IAMDomainA",
            "agency_name": "IAMAgency",
            "duration_seconds": 3600
         }
      }
   }
}
```

Example Response

Status code: 201

The request is successful.

The responses to all the preceding requests are the same regardless of whether **session_user** is specified or not. If **session_user** is specified, the security token contains the corresponding enterprise user information.

```
{
    "credential": {
        "access": "E6DX0TF2ZREQ4Z...",
        "expires_at": "2020-01-08T02:56:19.587000Z",
        "secret": "w9ePum0qdfac39ErLD0UdjofYkqort6Iw....",
        "securitytoken": "gQpjbi1ub3J0aC0..."
    }
}
```

Status Codes

Status Code	Description
201	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
500	Internal server error.

Error Codes

None

5.2.2 Obtaining a Temporary Access Key and Security Token Through a Token

Function

This API is used to obtain a temporary access key and a security token through a token. Temporary access keys and security tokens are issued by the system to IAM users, and can be valid for 15 minutes to 24 hours. Temporary access keys and security tokens are granted with the least privilege.

The API can be called using both the global endpoint and region-specific endpoints.

A temporary access key must be used together with a security token, and the **x-security-token** field must be included in the request header. For details, see **How Do I Use a Temporary AK/SK to Sign Requests?**

URI

POST /v3.0/OS-CREDENTIAL/securitytokens

Request Parameters

Table 5-93 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token, federated user token, or agency token.

Table 5-94 Parameters in the request body

Parameter	Mandatory	Type	Description
auth	Yes	Object	Authentication information.

Table 5-95 auth

Parameter	Mandatory	Type	Description
identity	Yes	Object	Authentication parameters.

Table 5-96 auth.identity

Parameter	Mandatory	Type	Description
methods	Yes	Array of strings	Authentication method. The value of this field is **["token"]**.
token	No	Object	Validity period of a temporary access key and security token.

Parameter	Mandatory	Type	Description
policy	No	Object	Permissions to be assigned to the temporary access key and security token (currently the policy only applies to OBS). The final permissions of the temporary access key and security token are the intersection of permissions assigned to the specified user token and defined in this parameter. For details about the format and syntax of IAM policies, see **Policies**.

Table 5-97 auth.identity.policy

Parameter	Mandatory	Type	Description
Version	Yes	String	Policy version. When creating a custom policy, set this parameter to **1.1**. **NOTE** **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Yes	Array of objects	Statement of the policy.

Table 5-98 auth.identity.policy.Statement

Parameter	Mandatory	Type	Description
Action	Yes	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations.
Effect	Yes	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny
Condition	No	Map<String,Map<String,Array<String>>>	Conditions for the permission to take effect. For details, see **Policy Syntax**. **NOTE** In the following request example, the policy is in effect only when **DomainName** is set to **DomainNameExample**. `"Condition": { "StringEquals": { "g:DomainName": [ "DomainNameExample" ] } }`

Parameter	Mandatory	Type	Description
Resource	No	Array of strings	Cloud resource. **NOTE** • Format: *Service name*:*Region*:*Domain ID*:*Resource type*:*Resource path*. Wildcard characters (*) are supported. For example, **obs:*:*:bucket:*** means all OBS buckets. For details about cloud services that support resource-level authorization, see **Cloud Services Supported by IAM**. • The region segment can be * or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • The service name, region, domain ID, and resource type can be 1 to 50 characters long, including letters, digits, underscores (_), hyphens (-), and asterisks (*). The resource path can be 1 to 1200 characters long, excluding semicolons (;), vertical bars (|), tildes (~), backquote (`), curly brackets ({}), square brackets ([]), and angle brackets (<>).

Table 5-99 auth.identity.token

Parameter	Mandatory	Type	Description
id	No	String	Token. This parameter is mandatory if **X-Auth-Token** is not specified in the request header.
duration_seconds	No	Integer	Validity period (in seconds) of a temporary access key and security token. The value ranges from 15 minutes to 24 hours. The default value is 15 minutes.

Response Parameters

Table 5-100 Parameters in the response body

Parameter	Type	Description
credential	Object	Authentication result.

Table 5-101 credential

Parameter	Type	Description
expires_at	String	Expiration time of the access key and security token. The response is UTC time.
access	String	AK.
secret	String	SK.
securitytoken	String	Obtained access key in ciphertext.

Example Request

- Request with **token** (specifying the validity period of a temporary access key and security token)

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/securitytokens
{
    "auth": {
        "identity": {
            "methods": [
                "token"
            ],
            "token": {
                "id": "MIIEIgYJKoZIhvc...",
                "duration_seconds": "900"
            }
        }
    }
}
```

- Request with the **X-Auth-Token** header but without the **token** parameter

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/securitytokens
{
    "auth": {
        "identity": {
            "methods": [
                "token"
            ]
        }
    }
}
```

- Request with **policy** set to control the permissions assigned to the obtained temporary access key and security token (currently the policy applies only to OBS). The final permissions of the temporary access key and security token are the intersection of permissions assigned to the specified user token and defined in this parameter.

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/securitytokens
{
  "auth": {
```

```
  "identity": {
    "methods": [
      "token"
    ],
    "policy": {
      "Version": "1.1",
      "Statement": [
        {
          "Effect": "Allow",
          "Action": [
            "obs:object:GetObject"
          ],
          "Resource": [
            "OBS:*:*:object:*"
          ],
          "Condition": {
            "StringEquals": {
              "g:DomainName": [
                "DomainNameExample"                    //Example condition value. Replace it with the
actual value.
              ]
            }
          }
        }
      ]
    },
    "token": {
      "duration_seconds": 900
    }
  }
 }
}
```

Example Response

Status code: 201

The request is successful.

```
{
   "credential": {
      "access": "NZFAT5VNWEJDGZ4PZ...",
      "expires_at": "2020-01-08T03:50:07.574000Z",
      "secret": "riEoWsy3qO0BvgwfkoLVgCUvzgpjBBcvdq...",
      "securitytoken": "gQpjbi1ub3J0aC00jD4Ej..."
   }
}
```

Status Codes

Status Code	Description
201	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
500	Internal server error.

Error Codes

None

5.2.3 Creating a Permanent Access Key

Function

This API can be used by the **administrator** to create a permanent access key for an IAM user or used by an IAM user to create a permanent access key.

Access keys are identity credentials for using development tools (APIs, CLI, and SDKs) to access Huawei Cloud. Access keys cannot be used to log in to the console. AK is used in conjunction with an SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct. For details about how to create an access key on the console, see **Access Keys**.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3.0/OS-CREDENTIAL/credentials

Request Parameters

Table 5-102 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	If an **administrator** is requesting to create a permanent access key for an IAM user, see **Actions**. If an IAM user is requesting to create a permanent access key, the user token (no special permission requirements) of the user is required.

Table 5-103 Parameters in the request body

Parameter	Mandatory	Type	Description
credential	Yes	Object	Authentication information.

Table 5-104 credential

Parameter	Mandatory	Type	Description
user_id	Yes	String	ID of the IAM user who is requesting to create an access key. For details about how to obtain the user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
description	No	String	Description of the access key.

Response Parameters

Table 5-105 Parameters in the response body

Parameter	Type	Description
credential	Object	Authentication result.

Table 5-106 credential

Parameter	Type	Description
create_time	String	Time when the access key was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
access	String	AK.
secret	String	SK.
status	String	Status of the access key. Options: • **active**: Enabled • **inactive**: Disabled
user_id	String	IAM user ID.
description	String	Description of the access key.

Example Request

Request for creating a permanent access key for an IAM user whose ID is 07609fb9358010e21f7bc003751c7c32

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials
{
    "credential": {
        "description": "IAMDescription",
        "user_id": "07609fb9358010e21f7bc003751c7c32"
    }
}
```

Example Response

Status code: 201

The permanent access key is created successfully.

```
{
    "credential": {
        "access": "P83EVBZJMXCYTMUII...",
        "create_time": "2020-01-08T06:25:19.014028Z",
        "user_id": "07609fb9358010e21f7bc003751...",
        "description": "IAMDescription",
        "secret": "TTqAHPbhWorg9ozx8Dv9MUyzYnOKDppxzHt...",
        "status": "active"
    }
}
```

Status code: 400

Invalid parameters. (The number of access keys has reached the maximum allowed limit.)

```
{
    "error": {
        "message": "akSkNumExceed",
        "code": 400,
        "title": "Bad Request"
    }
}
```

Status Codes

Status Code	Description
201	The permanent access key is created successfully.
400	Invalid parameters, or the number of access keys has reached the maximum allowed limit.
401	Authentication failed.
403	Access denied.
500	Internal server error.

Error Codes

None

5.2.4 Querying Permanent Access Keys

Function

This API can be used by the **administrator** to query all permanent access key of an IAM user or used by an IAM user to query all of their own permanent access keys.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-CREDENTIAL/credentials

Table 5-107 Query parameters

Parameter	Mandatory	Type	Description
user_id	No	String	User ID.

Request Parameters

Table 5-108 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	If an IAM user is requesting to query their own permanent access keys, the user token (no special permission requirements) of the user is required. If the **administrator** is requesting to query all permanent access keys of an IAM user, see **Actions**.

Response Parameters

Table 5-109 Parameters in the response body

Parameter	Type	Description
credentials	Array of objects	Authentication result.

Table 5-110 credentials

Parameter	Type	Description
user_id	String	IAM user ID.
access	String	AK.
status	String	Status of the access key. Options: • **active**: Enabled • **inactive**: Disabled
create_time	String	Time when the access key was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.
description	String	Description of the access key.

Example Request

- Request for an IAM user to query their own permanent access keys
  ```
  GET https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials
  ```
- Request for an administrator to query all permanent access keys of an IAM user (user ID: **07609fb9358010e21f7bc003751c...**)
  ```
  GET https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials?
  user_id=07609fb9358010e21f7bc0037....
  ```

Example Response

Status code: 200

The request is successful.

```
{
  "credentials": [
    {
      "access": "LOSZM4YRVLKOY9E8X...",
      "create_time": "2020-01-08T06:26:08.123059Z",
      "user_id": "07609fb9358010e21f7bc0037...",
      "description": "",
      "status": "active"
```

```
    },
    {
        "access": "P83EVBZJMXCYTMU...",
        "create_time": "2020-01-08T06:25:19.014028Z",
        "user_id": "07609fb9358010e21f7bc003751...",
        "description": "",
        "status": "active"
    }
  ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.2.5 Querying a Permanent Access Key

Function

This API can be used by the **administrator** to query the specified permanent access key of an IAM user or used by an IAM user to query one of their own permanent access keys.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-CREDENTIAL/credentials/{access_key}

Table 5-111 URI parameters

Parameter	Mandatory	Type	Description
access_key	Yes	String	AK of the access key to be queried.

Request Parameters

Table 5-112 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	If the **administrator** is requesting to query a specified permanent access key of an IAM user, see **Actions**. If an IAM user is requesting to query one of their own permanent access keys, the user token (no special permission requirements) of the user is required.

Response Parameters

Table 5-113 Parameters in the response body

Parameter	Type	Description
credential	Object	Authentication result.

Table 5-114 credential

Parameter	Type	Description
user_id	String	IAM user ID.
access	String	AK.
status	String	Status of the access key. Options: • **active**: Enabled • **inactive**: Disabled
create_time	String	Time when the access key was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Parameter	Type	Description
last_use_time	String	The last time the access key was used. If the access key has never been used, the creation time of the access key is returned. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description	String	Description of the access key.

Example Request

Request for an IAM user to query their specific permanent access key

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials/{access_key}
```

Example Response

Status code: 200

The request is successful.

```
{
    "credential": {
        "last_use_time": "2020-01-08T06:26:08.123059Z",
        "access": "LOSZM4YRVLKOY9E8...",
        "create_time": "2020-01-08T06:26:08.123059Z",
        "user_id": "07609fb9358010e21f7bc003751...",
        "description": "",
        "status": "active"
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.2.6 Modifying a Permanent Access Key

Function

This API can be used by the **administrator** to modify the specified permanent access key of an IAM user or used by an IAM user to modify one of their own permanent access keys.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-CREDENTIAL/credentials/{access_key}

Table 5-115 URI parameters

Parameter	Mandatory	Type	Description
access_key	Yes	String	AK of the access key to be modified.

Request Parameters

Table 5-116 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	If the **administrator** is requesting to modify a specified permanent access key of an IAM user, see **Actions**. If an IAM user is requesting to modify one of their own permanent access keys, the user token (no special permission requirements) of the user is required.

Table 5-117 Parameters in the request body

Parameter	Mandatory	Type	Description
credential	Yes	Object	Authentication information.

Table 5-118 credential

Parameter	Mandatory	Type	Description
status	No	String	Status of the access key. Options: • **active**: Enabled • **inactive**: Disabled
description	No	String	Description of the access key.

Response Parameters

Table 5-119 Parameters in the response body

Parameter	Type	Description
credential	Object	Authentication information.

Table 5-120 credential

Parameter	Type	Description
user_id	String	IAM user ID.
access	String	AK.
status	String	Status of the access key. Options: • **active**: Enabled • **inactive**: Disabled
create_time	String	Time when the access key was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.
description	String	Description of the access key.

Example Request

Request for an IAM user to disable their specific permanent access key

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials/{access_key}
{
    "credential": {
```



```
    "status": "inactive",
    "description": "IAMDescription"
  }
}
```

Example Response

Status code: 200

The request is successful.

```
{
  "credential": {
    "status": "inactive",
    "access": "LOSZM4YRVLKOY9...",
    "create_time": "2020-01-08T06:26:08.123059Z",
    "user_id": "07609fb9358010e21f7bc00375..."
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.2.7 Deleting a Permanent Access Key

Function

This API can be used by the **administrator** to delete the specified permanent access key of an IAM user or used by an IAM user to delete one of their own permanent access keys.

The API can be called using both the global endpoint and region-specific endpoints.

NOTE

Deleted permanent access keys cannot be recovered. Check that the access keys have not been used for more than one week before deleting them.

URI

DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key}

Table 5-121 URI parameters

Parameter	Mandatory	Type	Description
access_key	Yes	String	AK to be deleted.

Request Parameters

Table 5-122 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	If the **administrator** is requesting to delete a specified permanent access key of an IAM user, see **Actions**. If an IAM user is requesting to delete one of their own permanent access keys, the user token (no special permission requirements) of the user is required.

Response Parameters

None

Example Request

Request for deleting a permanent access key

```
DELETE https://iam.myhuaweicloud.eu/v3.0/OS-CREDENTIAL/credentials/{access_key}
```

Example Response

None

Status Codes

Status Code	Description
204	The access key is deleted successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.3 Region Management

5.3.1 Querying Regions

Function

This API is used to query the regions accessible to a specified user.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/regions

Request Parameters

Table 5-123 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token (no special permission requirements). If the token does not contain private region information, no private regions will be returned.

Response Parameters

Table 5-124 Parameters in the response body

Parameter	Type	Description
links	Object	Resource link information.
regions	Array of objects	Region information.

Table 5-125 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-126 regions

Parameter	Type	Description
description	String	Description of the region.
parent_region_id	String	Null.
links	Object	Region resource link.
locales	Object	Region name.
id	String	Region ID.
type	String	Region type.

Table 5-127 regions.links

Parameter	Type	Description
self	String	Resource link.

Table 5-128 regions.locales

Parameter	Type	Description
zh-cn	String	Region name in Chinese.

Parameter	Type	Description
en-us	String	Region name in English.
pt-br	String	Region name in Portuguese.
es-us	String	Region name in American Spanish.
es-es	String	Region name in Spanish.

Example Request

Request for querying a region list

```
GET https://iam.myhuaweicloud.eu/v3/regions
```

Example Response

Status code: 200

The request is successful.


```
{
   "regions": [
      {
         "parent_region_id": null,
         "description": "",
         "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/regions/eu-west-101"
         },
         "type": "public",
         "id": "eu-west-101",
         "locales": {
            "zh-cn": "EU-Dublin",
            "en-us": "eu-west-101"
         }
      },
      {
         "parent_region_id": null,
         "description": "",
         "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/regions/la-south-2"
         },
         "type": "public",
         "id": "la-south-2",
         "locales": {
            "pt-br": "AL-Santiago",
            "zh-cn": "Region name in Chinese",
            "en-us": "LA-Santiago",
            "es-us": "AL-Santiago de Chile1",
            "es-es": "LA-Santiago"
         }
      }
   ],
   "links": {
      "self": "https://iam.myhuaweicloud.eu/v3/regions",
      "previous": null,
      "next": null
   }
}
```


Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.3.2 Querying Region Details

Function

This API is used to query region details.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/regions/{region_id}

Table 5-129 URI parameters

Parameter	Mandatory	Type	Description
region_id	Yes	String	ID of the region to be queried. You can obtain a region ID by using the API described in **Querying Regions** or **using the console**.

Request Parameters

Table 5-130 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token (no special permission requirements).

Response Parameters

Table 5-131 Parameters in the response body

Parameter	Type	Description
region	Object	Region information.

Table 5-132 region

Parameter	Type	Description
description	String	Description of the region.
parent_region_id	String	Null.
links	Object	Region resource link.
locales	Object	Region name.
id	String	Region ID.
type	String	Region type.

Table 5-133 region.links

Parameter	Type	Description
self	String	Resource link.

Table 5-134 region.locales

Parameter	Type	Description
zh-cn	String	Region name in Chinese.
en-us	String	Region name in English.
pt-br	String	Region name in Portuguese.
es-us	String	Region name in American Spanish.
es-es	String	Region name in Spanish.

Example Request

Request for querying region details

```
GET https://iam.myhuaweicloud.eu/v3/regions/{region_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "region": {
        "description": "",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/regions/la-south-2"
        },
        "type": "public",
        "id": "la-south-2",
        "locales": {
            "pt-br": "AL-Santiago",
            "zh-cn": "Region name in Chinese",
            "en-us": "LA-Santiago",
            "es-us": "AL-Santiago de Chile1",
            "es-es": "LA-Santiago"
        }
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Status Code	Description
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.4 Project Management

5.4.1 Querying Project Information

Function

This API is used to query project information.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/projects

Table 5-135 Query parameters

Parameter	Mandatory	Type	Description
domain_id	No	String	Account ID of the target project. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
enabled	No	Boolean	Enabling status of the project.
is_domain	No	Boolean	Leave this field blank.

Parameter	Mandatory	Type	Description
name	No	String	Project name. For details about how to obtain the project name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
page	No	Integer	Page number for pagination query. The minimum value is **1**. This parameter must be used together with **per_page**.
parent_id	No	String	Specify the ID of a subproject. Alternatively, specify the account ID of a system project, for example, the eu-west-101 project. For details about how to obtain the project ID and account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
per_page	No	Integer	Number of data records to be displayed on each page. The value ranges from 1 to 5000. This parameter must be used together with **page**.

Request Parameters

Table 5-136 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-137 Parameters in the response body

Parameter	Type	Description
links	Object	Resource link information.
projects	Array of objects	Project information.

Table 5-138 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-139 projects

Parameter	Type	Description
is_domain	Boolean	The value is **false**.
description	String	Description of the project.
links	Object	Project resource link.
enabled	Boolean	Enabling status of the project.
id	String	Project ID.
parent_id	String	ID of the specified subproject or account ID of a specified system project, for example, the **eu-west-101** project.
domain_id	String	Account ID.
name	String	Project name. For example, **eu-west-101** and **MOS**. MOS is a built-in project of OBS.

Table 5-140 projects.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.

Parameter	Type	Description
next	String	Next resource link.

Example Request

Request for querying project information

```
GET https://iam.myhuaweicloud.eu/v3/projects
```

Example Response

Status code: 200

The request is successful.

```
{
   "projects": [
      {
         "domain_id": "d78cbac186b744899480f25bd02...",
         "is_domain": false,
         "parent_id": "d78cbac186b744899480f25bd022...",
         "name": "eu-west-101",
         "description": "",
         "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/projects/06f1c15e6f0010672f86c003006c5f17"
         },
         "id": "06f1c15e6f0010672f86c00300...",
         "enabled": true
      },
      {
         "domain_id": "d78cbac186b744899480f25bd...",
         "is_domain": false,
         "parent_id": "d78cbac186b744899480f25bd0...",
         "name": "",
         "description": "",
         "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/projects/065a7c66da0010992ff7c0031e5a..."
         },
         "id": "065a7c66da0010992ff7c0031e5a...",
         "enabled": true
      }
   ],
   "links": {
      "next": null,
      "previous": null,
      "self": "https://iam.myhuaweicloud.eu/v3/projects"
   }
}
```

Status Codes

Status Code	Description
200	The request is successful.

Status Code	Description
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.4.2 Listing Projects

Function

This API can be used by the **administrator** to list the projects accessible to a specified IAM user or used by an IAM user to list accessible projects.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/users/{user_id}/projects

Table 5-141 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-142 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. If the **administrator** is requesting to list the projects of a specified IAM user. see **Actions**. If an IAM user is requesting to list accessible projects, the user token (no special permission requirements) of the user is required.

Response Parameters

Table 5-143 Parameters in the response body

Parameter	Type	Description
links	Object	Resource link information.
projects	Array of objects	Project information.

Table 5-144 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-145 projects

Parameter	Type	Description
is_domain	Boolean	The value is **false**.
description	String	Description of the project.
links	Object	Project resource link.

Parameter	Type	Description
enabled	Boolean	Enabling status of the project.
id	String	Project ID.
parent_id	String	ID of the specified subproject or account ID of a specified system project, for example, the **eu-west-101** project.
domain_id	String	Account ID of the project.
name	String	Project name.

Table 5-146 projects.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying project information of a specified IAM user

```
GET https://iam.myhuaweicloud.eu/v3/users/{user_id}/projects
```

Example Response

Status code: 200

The request is successful.

```
{
   "projects": [
      {
         "domain_id": "d78cbac186b744899480f25bd02...",
         "is_domain": false,
         "parent_id": "d78cbac186b744899480f25bd0...",
         "name": "eu-west-101",
         "description": "",
         "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/projects/06f1cd8ea9800ff02f26c003d93..."
         },
         "id": "06f1cd8ea9800ff02f26c003d93...",
         "enabled": true
      },
      {
         "domain_id": "d78cbac186b744899480f25bd02...",
         "is_domain": false,
         "parent_id": "d78cbac186b744899480f25bd0...",
         "name": "MOS",
         "description": "",
```



```
            "links": {
                "next": null,
                "previous": null,
                "self": "https://iam.myhuaweicloud.eu/v3/projects/babf0605d15b4f9fbcacc6a8ee0f8d84"
            },
            "id": "babf0605d15b4f9fbcacc6a8ee0f8d84",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://iam.myhuaweicloud.eu/v3/users/7116d09f88fa41908676fdd4b039e95b/projects"
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.4.3 Listing Projects Accessible to an IAM User

Function

This API is used to list the projects in which resources are accessible to a specified IAM user.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/auth/projects

Request Parameters

Table 5-147 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token (no special permission requirements)

Response Parameters

Table 5-148 Parameters in the response body

Parameter	Type	Description
links	Object	Resource link information.
projects	Array of objects	Project information.

Table 5-149 links

Parameter	Type	Description
self	String	Resource link.

Table 5-150 projects

Parameter	Type	Description
is_domain	Boolean	The value is **false**.
description	String	Description of the project.
links	Object	Project resource link.
enabled	Boolean	Enabling status of the project.
id	String	Project ID.
parent_id	String	ID of the specified subproject or account ID of a specified system project, for example, the **eu-west-101** project.
domain_id	String	ID of the account to which the project belongs.
name	String	Project name.

Table 5-151 projects.links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for querying the projects accessible to a specified IAM user

```
GET https://iam.myhuaweicloud.eu/v3/auth/projects
```

Example Response

Status code: 200

The request is successful.

```
{
  "projects": [
    {
      "domain_id": "d78cbac186b744899480f25bd02...",
      "is_domain": false,
      "parent_id": "d78cbac186b744899480f25bd022...",
      "name": "af-south-1",
      "description": "",
      "links": {
        "self": "https://iam.myhuaweicloud.eu/v3/projects/06f1cbbaf280106b2f14c00313a9d065"
      },
      "id": "06f1cbbaf280106b2f14c00313a9...",
      "enabled": true
    },
    {
      "domain_id": "d78cbac186b744899480f25bd02...",
      "is_domain": false,
      "parent_id": "d78cbac186b744899480f25bd022...",
      "name": "",
      "description": "",
      "links": {
        "self": "https://iam.myhuaweicloud.eu/v3/projects/065a7c66da0010992ff7c0031e5a5e7d"
      },
      "id": "065a7c66da0010992ff7c0031e5a5e7d",
      "enabled": true
    }
  ],
  "links": {
    "self": "https://iam.myhuaweicloud.eu/v3/auth/projects"
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.

Status Code	Description
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.4.4 Creating a Project

Function

This API is provided for the **administrator** to create a project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3/projects

Request Parameters

Table 5-152 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-153 Parameters in the request body

Parameter	Mandatory	Type	Description
project	Yes	Object	Project information.

Table 5-154 project

Parameter	Mandatory	Type	Description
name	Yes	String	Project name, which must start with *ID of an existing region*_ and can contain less than or equal to 64 characters. For example, the ID of the **EU-Dublin** region is **eu-west-101**. You can create a subproject named **eu-west-101_IAMProject** in this region.
parent_id	Yes	String	Project ID of the corresponding region. For example, the project ID of the **EU-Dublin** region is **04dd42abe48026ad2fa3c01ad7fa.....**. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_id	No	String	ID of the account to which the project belongs.
description	No	String	Project description, which can contain a maximum of 255 characters.

Response Parameters

Table 5-155 Parameters in the response body

Parameter	Type	Description
project	Object	Project information.

Table 5-156 project

Parameter	Type	Description
is_domain	Boolean	The value is **false**.
description	String	Description of the project.
links	Object	Project resource link.
enabled	Boolean	Enabling status of the project.
id	String	Project ID.
parent_id	String	Project ID of the corresponding region. For example, the project ID of the **EU-Dublin** region is **04dd42abe48026ad2fa3c01ad7fa.....**
domain_id	String	Account ID of the project.
name	String	Project name.

Table 5-157 project.links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for creating a project named **eu-west-101_IAMProject** under the account whose ID is **d78cbac186b744899480f25bd0...** in the EU-Dublin region

```
POST https://iam.myhuaweicloud.eu/v3/projects
{
    "project": {
        "name": "eu-west-101_IAMProject",
        "parent_id": "aa2d97d7e62c4b7da3ffdfc11551f878",
        "domain_id": "d78cbac186b744899480f25bd0...",
        "description": "IAMDescription"
    }
}
```

Example Response

Status code: 201

The project is created successfully.

```
{
    "project": {
        "is_domain": false,
        "description": "IAMDescription",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/projects/07707ab14980265e2f5fc003a021bbc3"
        },
        "enabled": true,
        "id": "07707ab14980265e2f5fc003a021bbc3",
```

```
        "parent_id": "aa2d97d7e62c4b7da3ffdfc11551f878",
        "domain_id": "d78cbac186b744899480f25bd02...",
        "name": "eu-west-101_IAMProject"
    }
}
```

Status Codes

Status Code	Description
201	The project is created successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
409	A resource conflict occurs.

Error Codes

None

5.4.5 Modifying Project Information

Function

This API is provided for the **administrator** to modify project information.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PATCH /v3/projects/{project_id}

Table 5-158 URI parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	ID of the project to be modified. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-159 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-160 Parameters in the request body

Parameter	Mandatory	Type	Description
project	Yes	Object	Project information.

Table 5-161 project

Parameter	Mandatory	Type	Description
name	No	String	Project name, which must start with *ID of an existing region*_ and can contain less than or equal to 64 characters. The region to which the project belongs cannot be changed. For example, if the original project name is **eu-west-101_IAMProject**, the new project name must also start with **eu-west-101**_. Either **name** or **description** must be specified.
description	No	String	Project description, which can contain a maximum of 255 characters. Either **name** or **description** must be specified.

Response Parameters

Table 5-162 Parameters in the response body

Parameter	Type	Description
project	Object	Project information.

Table 5-163 project

Parameter	Type	Description
is_domain	Boolean	The value is **false**.
description	String	Description of the project.
extra	Object	Additional information about the project.
links	Object	Project resource link.
enabled	Boolean	Enabling status of the project.
id	String	Project ID.
parent_id	String	Project ID of the corresponding region. For example, the project ID of the **EU-Dublin** region is **04dd42abe48026ad2fa3c01ad7fa.....**
domain_id	String	Account ID of the project.
name	String	Project name.

Table 5-164 project.links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for changing the project name to **eu-west-101_IAMNewProject** and description to **IAMDescription**

```
PATCH https://iam.myhuaweicloud.eu/v3/projects/{project_id}
{
    "project": {
        "name": "eu-west-101_IAMNewProject",
        "description": "IAMDescription"
    }
}
```

Example Response

Status code: 200

The request is successful.


```
{
    "project": {
        "is_domain": false,
        "description": "IAMDescription",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/projects/07707ab14980265e2f5fc003a021bbc3"
        },
        "extra": {},
        "enabled": true,
        "id": "07707ab14980265e2f5fc003a021bbc3",
        "parent_id": "aa2d97d7e62c4b7da3ffdfc11551f878",
        "domain_id": "d78cbac186b744899480f25bd...",
        "name": "eu-west-101_IAMNewProject"
    }
}
```


Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
409	A resource conflict occurs.

Error Codes

None

5.4.6 Querying Project Information

Function

This API is used to query the detailed information about a project based on the project ID.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/projects/{project_id}

Table 5-165 URI parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	ID of the project to be queried. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-166 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token (no special permission requirements).

Response Parameters

Table 5-167 Parameters in the response body

Parameter	Type	Description
project	Object	Project information.

Table 5-168 project

Parameter	Type	Description
is_domain	Boolean	The value is **false**.
description	String	Description of the project.
links	Object	Project resource link.
enabled	Boolean	Enabling status of the project.
id	String	Project ID.
parent_id	String	ID of the specified subproject or account ID of a specified system project, for example, the **eu-west-101** project.

Parameter	Type	Description
domain_id	String	Account ID of the project.
name	String	Project name.

Table 5-169 project.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying project information

```
GET https://iam.myhuaweicloud.eu/v3/projects/{project_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "project": {
        "is_domain": false,
        "description": "",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/projects/2e93d63d8d2249f5a4ac5e2c78586a6e"
        },
        "enabled": true,
        "id": "2e93d63d8d2249f5a4ac5e2c78586a6e",
        "parent_id": "44c0781c83484eb9a4a5d4d233522cea",
        "domain_id": "44c0781c83484eb9a4a5d4d23...",
        "name": "MOS"
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.

Status Code	Description
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.4.7 Changing Project Status

Function

This API is provided for the **administrator** to change the status of a specified project. The project status can be normal or suspended.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3-ext/projects/{project_id}

Table 5-170 URI parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-171 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-172 Parameters in the request body

Parameter	Mandatory	Type	Description
project	Yes	Object	Project information.

Table 5-173 project

Parameter	Mandatory	Type	Description
status	Yes	String	Project status. The value can be **suspended** or **normal**. • **suspended**: Freeze the project. • **normal**: Unfreeze the project. Options: • suspended • normal

Response Parameters

None

Example Request

Request for changing the project status to **suspended**

```
PUT https://iam.myhuaweicloud.eu/v3-ext/projects/{project_id}
{
    "project": {
        "status": "suspended"
    }
}
```

Example Response

None

Status Codes

Status Code	Description
204	Setting successful.

Status Code	Description
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.4.8 Querying Project Information and Status

Function

This API is provided for the **administrator** to query project details and status.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3-ext/projects/{project_id}

Table 5-174 URI parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	ID of the project to be queried. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-175 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Token with **Security Administrator** permissions.

Response Parameters

Table 5-176 Parameters in the response body

Parameter	Type	Description
project	Object	Project information.

Table 5-177 project

Parameter	Type	Description
domain_id	String	ID of the account to which the project belongs.
is_domain	Boolean	The value is **false**.
parent_id	String	ID of the specified subproject or account ID of a specified system project, for example, the **eu-west-101** project.
name	String	Project name.
description	String	Description of the project.
id	String	Project ID.
enabled	Boolean	Enabling status of the project.
status	String	Project status.

Example Request

Request for querying project information and status

```
GET https://iam.myhuaweicloud.eu/v3-ext/projects/{project_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "project": {
        "domain_id": "d78cbac186b744899480f25bd02...",
        "is_domain": false,
        "parent_id": "aa2d97d7e62c4b7da3ffdfc11551...",
        "name": "eu-west-101_IAMProject",
        "description": "IAMDescription",
        "id": "07707ab14980265e2f5fc003a02...",
        "enabled": true,
        "status": "normal"
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.4.9 Querying the Quotas of a Project

Function

This API is used to query the quotas of a specified project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-QUOTA/projects/{project_id}

Table 5-178 URI parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	ID of the project to be queried. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-179 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	A token with Security Administrator permissions or an IAM user token. (No special permissions are required, but the scope of the token must be the project specified in the URL.)

Response Parameters

Table 5-180 Parameters in the response body

Parameter	Type	Description
quotas	object	Quota information of the account.

Table 5-181 quotas

Parameter	Type	Description
resources	Array of objects	Resource information.

Table 5-182 resources

Parameter	Type	Description
max	Integer	Maximum quota.

Parameter	Type	Description
min	Integer	Minimum quota.
quota	Integer	Current quota.
type	String	Quota type.
used	Integer	Used quota.

Example Request

Request for querying the project quota

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-QUOTA/projects/{project_id}
```

Example Response

Status code: 200

The request is successful.

```
{
  "quotas" : {
              "resources" : [
                   {
                        "max" : 50,
                        "min" : 0,
                        "quota" : 10,
                        "type" : "project",
                        "used" : 4
                     }
                  ]
            }
}
```

Status code: 403

Access denied.

- Example 1

```
{
   "error_msg" : "You are not authorized to perform the requested action.",
   "error_code" : "IAM.0002"
 }
```

- Example 2

```
{
   "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
   "error_code" : "IAM.0003"
 }
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal server error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.5 Account Management

5.5.1 Querying Account Information Accessible to an IAM User

Function

This API is used to query the account information that is accessible to a specified IAM user.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/auth/domains

Request Parameters

Table 5-183 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM user token (no special permission requirements).

Response Parameters

Table 5-184 Parameters in the response body

Parameter	Type	Description
domains	Array of objects	Account information.
links	Object	Resource link information.

Table 5-185 domains

Parameter	Type	Description
enabled	Boolean	Indicates whether an account is enabled. **true** (default value) indicates that the account is enabled. **false** indicates that the account is disabled.
id	String	Account ID.
name	String	Account name.
links	Object	Account resource link.
description	String	Description of the account.

Table 5-186 domains.links

Parameter	Type	Description
self	String	Resource link.

Table 5-187 links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for querying account information accessible to an IAM user

```
GET https://iam.myhuaweicloud.eu/v3/auth/domains
```

Example Response

Status code: 200

The request is successful.

```
{
    "domains": [
        {
            "description": "",
            "enabled": true,
            "id": "d78cbac186b744899480f25bd022f468",
            "links": {
                "self": "https://iam.myhuaweicloud.eu/v3/domains/d78cbac186b744899480f25bd022f468"
            },
            "name": "IAMDomain"
        }
    ],
    "links": {
        "self": "https://iam.myhuaweicloud.eu/v3/auth/domains"
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.5.2 Querying the Password Strength Policy

Function

This API is used to query the password strength policy, including the regular expression and description, of a specified account.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/domains/{domain_id}/config/security_compliance

Table 5-188 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-189 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Token (no special permission requirements) of the IAM user corresponding to the **domain_id** specified in the URL.

Response Parameters

Table 5-190 Parameters in the response body

Parameter	Type	Description
config	Object	Configuration information

Table 5-191 config

Parameter	Type	Description
security_compliance	Object	Password policy information

Table 5-192 config.security_compliance

Parameter	Type	Description
password_regex	String	Regular expression of the password strength policy
password_regex_description	String	Description of the password strength policy

Example Request

Request for querying the password strength policy

```
GET https://iam.myhuaweicloud.eu/v3/domains/{domain_id}/config/security_compliance
```

Example Response

Status code: 200

The request is successful.

```
{
    "config": {
        "security_compliance": {
            "password_regex": "^(?![A-Z]*$)(?![a-z]*$)(?![\\d]*$)(?![^\\W]*$)\\S{6,32}$",
            "password_regex_description": "The password must contain at least two of the following character types: uppercase letters, lowercase letters, digits, and special characters, and be a length between 6 and 32."
        }
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Status Code	Description
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.5.3 Querying the Regular Expression or Description of a Password Strength Policy

Function

This API is used to query the password strength policy, including the regular expression and description, of a specified account based on specified conditions.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/domains/{domain_id}/config/security_compliance/{option}

Table 5-193 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Parameter	Mandatory	Type	Description
option	Yes	String	Query condition, which can be **password_regex** or **password_regex_description**. **password_regex** indicates the regular expression of the password strength policy, and **password_regex_description** indicates the description of the password strength policy. Options: • password_regex • password_regex_description

Request Parameters

Table 5-194 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Token (no special permission requirements) of the IAM user corresponding to the **domain_id** specified in the URL.

Response Parameters

Table 5-195 Parameters in the response body

Parameter	Type	Description
config	Object	Configuration information.

Table 5-196 config

Parameter	Type	Description
password_regex	String	Regular expression of the password strength policy. (This parameter is returned if **option** is set to **password_regex**.)

Parameter	Type	Description
password_regex_description	String	Description of the password strength policy. (This parameter is returned if **option** is set to **password_regex_description**.)

Example Request

- Request for querying the password strength policy with **option** set to **password_regex**

  ```
  GET https://iam.myhuaweicloud.eu/v3/domains/{domain_id}/config/security_compliance/password_regex
  ```

- Request for querying the password strength policy with **option** set to **password_regex_description**

  ```
  GET https://iam.myhuaweicloud.eu/v3/domains/{domain_id}/config/security_compliance/password_regex_description
  ```

Example Response

Status code: 200

The request is successful.

Example 1: Response to the request with the **option** parameter being set to **password_regex**

Example 2: Response to the request with the **option** parameter being set to **password_regex_description**

- Example 1

  ```
  {
      "config": {
          "password_regex": "^(?![A-Z]*$)(?![a-z]*$)(?![\\d]*$)(?![^\\W]*$)\\S{6,32}$"
      }
  }
  ```

- Example 2

  ```
  {
      "config": {
          "password_regex_description": "The password must contain at least two of the following character types: uppercase letters, lowercase letters, digits, and special characters, and be a length between 6 and 32."
      }
  }
  ```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.

Status Code	Description
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.

Error Codes

None

5.5.4 Querying the Quotas of an Account

Function

This API is used to query the quotas of a specified account.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-QUOTA/domains/{domain_id}

Table 5-197 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Table 5-198 Query parameters

Parameter	Mandatory	Type	Description
type	No	String	Type of the quota you want to query. The options include: • **user**: IAM users • **group**: user groups • **idp**: identity providers • **agency**: agencies • **policy**: custom policies • **assigment_group_mp**: maximum number of permissions that can be assigned to a user group for an IAM project • **assigment_agency_mp**: maximum number of permissions that can be assigned to an agency • **assigment_group_ep**: maximum number of permissions that can be assigned to a user group for an enterprise project • **assigment_user_ep**: maximum number of permissions that can be assigned to a user for an enterprise project • **mapping**: mapping rule quota for all identity providers in the account

Request Parameters

Table 5-199 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	IAM user token (no special permission requirements).

Response Parameters

Status code: 200

Table 5-200 Parameters in the response body

Parameter	Type	Description
quotas	Object	Quota information of the account.

Table 5-201 quotas

Parameter	Type	Description
resources	Array of objects	Resource information.

Table 5-202 resources

Parameter	Type	Description
max	Integer	Maximum quota.
min	Integer	Minimum quota.
quota	Integer	Current quota.
type	String	Quota type.
used	Integer	Used quota. The number of used identity provider mapping rules is customized and is not returned.

Example Request

Request for querying the quotas of an account

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-QUOTA/domains/{domain_id}
```

Example Response

Status code: 200

The request is successful.

```
{
  "quotas" : {
    "resources" : [
            {
              "max" : 1000,
              "min" : 50,
              "quota" : 50,
              "type" : "user",
              "used" : 10
             },
            {
              "max" : 300,
              "min" : 10,
```

```
            "quota" : 20,
            "type" : "group",
            "used" : 8
          },
          {
            "max" : 20,
            "min" : 10,
            "quota" : 10,
            "type" : "idp",
            "used" : 9
          },
          {
            "max" : 300,
            "min" : 10,
            "quota" : 50,
            "type" : "agency",
            "used" : 12
          },
          {
            "max" : 300,
            "min" : 128,
            "quota" : 200,
            "type" : "policy",
            "used" : 8
          },
          {
            "max" : 500,
            "min" : 50,
            "quota" : 200,
            "type" : "assigment_group_mp",
            "used" : 8
          },
          {
            "max" : 500,
            "min" : 50,
            "quota" : 200,
            "type" : "assigment_agency_mp",
            "used" : 8
          },
          {
            "max" : 5000,
            "min" : 50,
            "quota" : 500,
            "type" : "assigment_group_ep",
            "used" : 8
          },
          {
            "max" : 5000,
            "min" : 50,
            "quota" : 500,
            "type" : "assigment_user_ep",
            "used" : 8
          },
          {
            "max" : 100,
            "min" : 10,
            "quota" : 10,
            "type" : "mapping",
            "used" : null
          }
        ]
      }
}
```


Status code: 400

Invalid parameters.


```
{
  "error_msg" : "Request parameter %(key)s is invalid.",
```

```
  "error_code" : "IAM.0007"
}
```

Status code: 403

Access denied.

- Example 1

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
  "error_code" : "IAM.0002"
}
```

- Example 2

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal server error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.6 IAM User Management

5.6.1 Listing IAM Users

Function

This API is provided for the **administrator** to list all IAM users.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/users

Table 5-203 Query parameters

Parameter	Mandatory	Type	Description
domain_id	No	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
enabled	No	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
name	No	String	IAM user name.

Parameter	Mandatory	Type	Description
password_expires_at	No	String	Password expiration time. The value **null** indicates that the password will never expire. Password format: **password_expires_at={operator}:{timestamp}**. Timestamp format: **YYYY-MM-DDTHH:mm:ssZ**. Example: password_expires_at=lt:2016-12-08T22:02:00Z **NOTE** • The value of **operator** can be **lt**, **lte**, **gt**, **gte**, **eq**, or **neq**. • **lt**: The expiration time is earlier than *timestamp*. • **lte**: The expiration time is earlier than or equal to *timestamp*. • **gt**: The expiration time is later than *timestamp*. • **gte**: The expiration time is equal to or later than *timestamp*. • **eq**: The expiration time is equal to *timestamp*. • **neq**: The expiration time is not equal to *timestamp*.

Request Parameters

Table 5-204 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-205 Parameters in the response body

Parameter	Type	Description
links	Object	Resource link information.
users	Array of objects	IAM user information.

Table 5-206 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-207 users

Parameter	Type	Description
name	String	IAM user name.
links	Object	IAM user resource link information.
domain_id	String	ID of the account to which the IAM user belongs.
enabled	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
id	String	IAM user ID.
password_expires_at	String	Password expiration time of the IAM user. If this parameter is set to **null**, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description	String	Description of the IAM user.
pwd_status	Boolean	Password status. **true** means that the password needs to be changed, and **false** means that the password is normal.

Parameter	Type	Description
last_project_id	String	ID of the project that the IAM user lastly accessed before exiting the system.
pwd_strength	String	Password strength. The value can be **high**, **mid**, or **low**.

Table 5-208 users.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for listing IAM users as an administrator

```
GET https://iam.myhuaweicloud.eu/v3/users
```

NOTE

To narrow down the query range, add a path parameter. For example:

```
GET https://iam.myhuaweicloud.eu/v3/users?
domain_id=d78cbac186b744899480f25bd02...&enabled=true
```

Example Response

Status code: 200

The request is successful.

```
{
  "links": {
    "next": null,
    "previous": null,
    "self": "https://iam.myhuaweicloud.eu/v3/users"
  },
  "users": [
    {
      "domain_id": "d78cbac186b744899480f25bd02...",
      "name": "IAMUserA",
      "description": "IAMDescriptionA",
      "password_expires_at": null,
      "links": {
        "next": null,
        "previous": null,
        "self": "https://iam.myhuaweicloud.eu/v3/users/07667db96a00265f1fc0c003a3..."
      },
      "id": "07667db96a00265f1fc0c003a...",
      "enabled": true
    },
    {
      "pwd_status": true,
```



```
        "domain_id": "d78cbac186b744899480f25bd02...",
        "last_project_id": "065a7c66da0010992ff7c0031e5a...",

        "name": "IAMUserB",
        "description": "IAMDescriptionB",
        "password_expires_at": null,
        "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/users/07609fb9358010e21f7bc003751c7..."
        },
        "id": "07609fb9358010e21f7bc003751c7...",
        "enabled": true
    }
  ]
}
```


Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	A resource conflict occurs.
500	The request entity is too large.
503	Service unavailable.

Error Codes

None

5.6.2 Querying IAM User Details (Recommended)

Function

This API can be used by the **administrator** to query the details about a specified IAM user or used by an IAM user to query their own details.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-USER/users/{user_id}

Table 5-209 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-210 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	If the **administrator** is requesting to query IAM user details, see **Actions**. If an IAM user is requesting to query their own details, the user token (no special permission requirements) of the user is required.

Response Parameters

Table 5-211 Parameters in the response body

Parameter	Type	Description
user	Object	IAM user information.

Table 5-212 user

Parameter	Type	Description
enabled	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
id	String	IAM user ID.
domain_id	String	ID of the account to which the IAM user belongs.
name	String	IAM user name.

Parameter	Type	Description
links	Object	IAM user resource link information.
xuser_id	String	ID of the IAM user in the external system.
xuser_type	String	Type of the IAM user in the external system.
areacode	String	Country code.
email	String	Email address.
phone	String	Mobile number.
pwd_status	Boolean	Password status. **true** means that the password needs to be changed, and **false** means that the password is normal.
update_time	String	Time when the IAM user was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.
create_time	String	Time when the IAM user was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.
last_login_time	String	Last login time of the IAM user. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.
pwd_strength	String	Password strength. The value can be **Low**, **Medium**, **Strong**, or **None**.
is_domain_owner	Boolean	Indicates whether the IAM user is an account administrator.
access_mode	String	Access type of the IAM user. • **default**: programmatic access and management console access. This option is the default access type. • **programmatic**: programmatic access • **console**: management console access
description	String	Description of the IAM user.

Table 5-213 user.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying IAM user details, including the mobile number and email address of the IAM user

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-USER/users/{user_id}
```

Example Response

Status code: 200

The request is successful.

```
{
  "user" : {
    "pwd_strength" : "Strong",
    "create_time" : "2020-07-08 02:19:03.0",
    "last_login_time" : null,
    "areacode" : "",
    "enabled" : true,
    "domain_id" : "086ba757f90089cf0fe5c000dbe7f...",
    "xuser_id" : "",
    "pwd_status" : false,
    "update_time" : null,
    "phone" : "-",
    "is_domain_owner" : false,
    "access_mode" : "default",
    "name" : "autotest1",
    "links" : {
      "next" : null,
      "previous" : null,
      "self" : "https://iam.myhuaweicloud.eu/v3.0/OS-USER/users/093f75808b8089ba1f6dc000c7cac..."
    },
    "id" : "093f75808b8089ba1f6dc000c7cac...",
    "xuser_type" : "",
    "email" : "",
    "description" : "aaa"
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
403	Access denied.
404	The requested resource cannot be found.

Status Code	Description
405	The method specified in the request is not allowed for the requested resource.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.6.3 Querying IAM User Details

Function

This API can be used by the **administrator** to query the details about a specified IAM user or used by an IAM user to query their own details.

The API can be called using both the global endpoint and region-specific endpoints.

Restrictions

This API cannot be used to query the mobile number and email address of an IAM user. To query such information, see **Querying IAM User Details (Recommended)**.

URI

GET /v3/users/{user_id}

Table 5-214 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-215 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	If the **administrator** is requesting to query IAM user details, see **Actions**. If an IAM user is requesting to query their own details, the user token (no special permission requirements) of the user is required.

Response Parameters

Table 5-216 Parameters in the response body

Parameter	Type	Description
user	Object	IAM user information.

Table 5-217 user

Parameter	Type	Description
name	String	IAM user name.
links	Object	IAM user resource link information.
domain_id	String	ID of the account to which the IAM user belongs.
enabled	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
id	String	IAM user ID.
password_expires_at	String	Password expiration time of the IAM user. If this parameter is set to **null**, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description	String	Description of the user.

Parameter	Type	Description
pwd_status	Boolean	Password status. **true** means that the password needs to be changed, and **false** means that the password is normal.
last_project_id	String	ID of the project that the IAM user lastly accessed before exiting the system.

Table 5-218 user.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying IAM user details, excluding the mobile number and email address of the IAM user

```
GET https://iam.myhuaweicloud.eu/v3/users/{user_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "user": {
        "pwd_status": true,
        "domain_id": "d78cbac186b744899480f25bd02...",
        "last_project_id": "065a7c66da0010992ff7c0031e5a5...",
        "name": "IAMUser",
        "description": "--",
        "password_expires_at": null,
        "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/users/07609fb9358010e21f7bc003751..."
        },
        "id": "7116d09f88fa41908676fdd4b039...",
        "enabled": true
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	A resource conflict occurs.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.6.4 Querying the User Groups to Which an IAM User Belongs

Function

This API can be used by the **administrator** to query the groups of a specified IAM user or used by an IAM user to query their own groups.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/users/{user_id}/groups

Table 5-219 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-220 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	If the **administrator** is requesting to query the groups to which an IAM user belongs, see **Actions**. If an IAM user is requesting to query their own groups, the user token (no special permission requirements) of the user is required.

Response Parameters

Table 5-221 Parameters in the response body

Parameter	Type	Description
groups	Array of objects	User group information.
links	Object	Resource link information.

Table 5-222 groups

Parameter	Type	Description
description	String	User group description.
id	String	User group ID.
domain_id	String	ID of the account to which the user group belongs.
name	String	User group name.
links	Object	User group resource link.
create_time	Long	Time when the user group was created.

Table 5-223 groups.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-224 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying the user groups to which an IAM user belongs

```
GET https://iam.myhuaweicloud.eu/v3/users/{user_id}/groups
```

Example Response

Status code: 200

The request is successful.

```
{
  "groups": [
    {
      "domain_id": "d78cbac186b744899480f25bd0...",
      "create_time": 1578107542861,
      "name": "IAMGroup",
      "description": "",
      "links": {
        "next": null,
        "previous": null,
        "self": "https://iam.myhuaweicloud.eu/v3/groups/07609e7eb200250a3f7dc003cb..."
      },
      "id": "07609e7eb200250a3f7dc003cb7..."
    }
  ],
  "links": {
    "next": null,
    "previous": null,
    "self": "https://iam.myhuaweicloud.eu/v3/users/076837351e80251c1f0fc003afe43.../groups"
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	A resource conflict occurs.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.6.5 Querying the IAM Users in a Group

Function

This API can be used by the **administrator** to query the IAM users in a user group.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/groups/{group_id}/users

Table 5-225 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-226 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-227 Parameters in the response body

Parameter	Type	Description
links	Object	User group resource link.
users	Array of objects	IAM user information.

Table 5-228 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-229 users

Parameter	Type	Description
name	String	IAM user name.
links	Object	IAM user resource link information.
domain_id	String	ID of the account to which the IAM user belongs.
enabled	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.

Parameter	Type	Description
id	String	IAM user ID.
password_expires_at	String	Password expiration time. If this parameter is set to **null**, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description	String	Description of the IAM user.
pwd_status	Boolean	Password status. **true** means that the password needs to be changed, and **false** means that the password is normal.
last_project_id	String	ID of the project that the IAM user lastly accessed before exiting the system.
pwd_strength	String	Password strength. The value can be **high**, **mid**, or **low**.
extra	object	Other information about the IAM user.

Table 5-230 users.extra

Parameter	Type	Description
description	string	Description of the IAM user.
last_project_id	string	ID of the project that the IAM user lastly accessed before exiting the system.
pwd_status	boolean	Password status. **true** means that the password needs to be changed, and **false** means that the password is normal.

Table 5-231 Users.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying the IAM users in a group

```
GET https://iam.myhuaweicloud.eu/v3/groups/{group_id}/users
```

Example Response

Status code: 200

The request is successful.

```
{
   "links": {
      "next": null,
      "previous": null,
      "self": "https://iam.myhuaweicloud.eu/v3/groups/07609e7eb200250a3f7dc003cb7a4e2d/users"
   },
   "users": [
      {
         "pwd_status": true,
         "domain_id": "d78cbac186b744899480f25bd...",
         "last_project_id": "065a7c66da0010992ff7c0031e...",
          "name": "IAMUserA",
         "description": "--",
         "password_expires_at": null,
         "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/users/07609fb9358010e21f7bc00375..."
         },
         "id": "07609fb9358010e21f7bc003751c7...",
         "enabled": true
      },
      {
         "pwd_status": true,
         "domain_id": "d78cbac186b744899480f25bd022...",
         "last_project_id": "065a7c66da0010992ff7c0031e5a...",
         "name": "IAMUserB",
         "description": "",
         "password_expires_at": null,
         "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/users/076837351e80251c1f0fc003af..."
         },
         "id": "076837351e80251c1f0fc003afe43...",
         "enabled": true
      }
   ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Invalid parameters.
403	Access denied.
404	The requested resource cannot be found.

Error Codes

None

5.6.6 Creating an IAM User (Recommended)

Function

This API is provided for the **administrator** to create an IAM user.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3.0/OS-USER/users

Request Parameters

Table 5-232 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access credential issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-233 Parameters in the request body

Parameter	Mandatory	Type	Description
user	Yes	Object	IAM user information.

Table 5-234 user

Parameter	Mandatory	Type	Description
name	Yes	String	IAM user name, which consists of 1 to 32 characters. It can contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.) and cannot start with a digit or space.
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
password	No	String	Password of the user. The password must meet the following requirements:
email	No	String	Email address with a maximum of 255 characters.
areacode	No	String	Country code. The country code must be used together with a mobile number.
phone	No	String	Mobile number with a maximum of 32 digits. The mobile number must be used together with a country code.
enabled	No	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
pwd_status	No	Boolean	Indicates whether password reset is required at the first login. By default, password reset is required.

Parameter	Mandatory	Type	Description
xuser_type	No	String	Type of the IAM user in the external system. The user type can contain a maximum of 64 characters. **xuser_type** must be used together with **xuser_id** and will be verified based on **xaccount_type** and **xdomain_type** of the same account. Currently, the parameter value can only be **TenantIdp**. **NOTE** An external system refers to an enterprise management system connected to Huawei Cloud. Parameters **xaccount_type**, **xaccount_id**, **xdomain_type**, **xdomain_id**, **xuser_type**, and **xuser_id** cannot be obtained from Huawei Cloud. Please contact your enterprise administrator.
xuser_id	No	String	ID of the IAM user in the external system. The user ID can contain a maximum of 128 characters, and must be used together with **xuser_type**. Due to the latency, the IAM console may not be able to display the external identity ID you have set in real time. Refresh the page later. **NOTE** An external system refers to an enterprise management system connected to Huawei Cloud. Parameters **xaccount_type**, **xaccount_id**, **xdomain_type**, **xdomain_id**, **xuser_type**, and **xuser_id** cannot be obtained from Huawei Cloud. Please contact your enterprise administrator.
access_mode	No	String	Access type of the IAM user. • **default**: programmatic access and management console access. This option is the default access type. • **programmatic**: programmatic access • **console**: management console access
description	No	String	Description of the IAM user.

Response Parameters

Table 5-235 Parameters in the response body

Parameter	Type	Description
user	Object	IAM user information.

Table 5-236 user

Parameter	Type	Description
status	Integer	Status of the IAM user.
pwd_status	Boolean	Indicates whether password reset is required at the first login.
xuser_id	String	ID of the IAM user in the external system. **NOTE** An external system refers to an enterprise management system connected to Huawei Cloud. Parameters **xaccount_type**, **xaccount_id**, **xdomain_type**, **xdomain_id**, **xuser_type**, and **xuser_id** cannot be obtained from Huawei Cloud. Please contact your enterprise administrator.
xuser_type	String	Type of the IAM user in the external system. **NOTE** An external system refers to an enterprise management system connected to Huawei Cloud. Parameters **xaccount_type**, **xaccount_id**, **xdomain_type**, **xdomain_id**, **xuser_type**, and **xuser_id** cannot be obtained from Huawei Cloud. Please contact your enterprise administrator.
access_mode	String	Access type of the IAM user. • **default**: programmatic access and management console access. This option is the default access type. • **programmatic**: programmatic access • **console**: management console access
description	String	Description of the IAM user.
name	String	IAM user name, which consists of 1 to 32 characters. It can contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.) and cannot start with a digit or space.
phone	String	Mobile number with a maximum of 32 digits. The mobile number must be used together with a country code.

Parameter	Type	Description
is_domain_owner	Boolean	Whether the IAM user is an **administrator**.
domain_id	String	ID of the account to which the IAM user belongs.
enabled	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
areacode	String	Country code.
email	String	Email address.
create_time	String	Time when the IAM user was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
xdomain_id	String	Customer code of the business entity.
xdomain_type	String	Business entity.
id	String	IAM user ID that contains 32 characters.
password_expires_at	String	Password expiration time. If this parameter is set to **null**, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Example Request

Request for an administrator to create an IAM user named **IAMUser**, with the email address **IAMEmail@huawei.com** and mobile number **0012312345678910** bound, and with both programmatic access and management console access

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-USER/users
{
    "user": {
        "domain_id": "d78cbac186b744899480f25...",
        "name": "IAMUser",
        "password": "IAMPassword@",
        "email": "IAMEmail@huawei.com",
        "areacode": "00123",
        "phone": "12345678910",
        "enabled": true,
        "pwd_status": false,
        "xuser_type": "",
        "xuser_id": "",
        "access_mode" : "default",
        "description": "IAMDescription"
```

```
    }
}
```

Example Response

Status code: 201

The IAM user is created successfully.

```
{
    "user": {
        "pwd_status": false,
        "xuser_id": "",
        "xuser_type": "",
        "access_mode" : "default",
        "description": "IAMDescription",
        "name": "IAMUser",
        "phone": "12345678910",
        "is_domain_owner": false,
        "enabled": true,
        "domain_id": "d78cbac186b744899480f25bd...",
        "areacode": "00123",
        "email": "IAMEmail@huaweiexample.com",
        "create_time": "2020-01-06T08:05:16.000000",
        "xdomain_id": "",
        "xdomain_type": "",
        "id": "07664aec578026691f00c003a..."
    }
}
```

Status Codes

Status Code	Description
201	The IAM user is created successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
409	A resource conflict occurs.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

See **Error Codes**.

5.6.7 Creating an IAM User

Function

This API is provided for the **administrator** to create an IAM user. An IAM user needs to change its password at the first login.

The API can be called using both the global endpoint and region-specific endpoints.

Restrictions

When you use this API to create an IAM user, you cannot specify a mobile number or email address for the IAM user. To specify a mobile number and email address, used the API described in **Creating an IAM User (Recommended)**.

URI

POST /v3/users

Request Parameters

Table 5-237 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-238 Parameters in the request body

Parameter	Mandatory	Type	Description
user	Yes	Object	User information.

Table 5-239 user

Parameter	Mandatory	Type	Description
name	Yes	String	IAM user name, which consists of 1 to 32 characters. It can contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.) and cannot start with a digit or space.
domain_id	No	String	ID of the account to which the IAM user belongs.
password	No	String	Password of the user. The password must meet the following requirements: • Can contain 6 to 32 characters. The default minimum password length is 6 characters. • Must contain at least two of the following character types: uppercase letters, lowercase letters, digits, and special characters. • Must meet the password requirements defined in the **password policy**.
enabled	No	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
description	No	String	Description of the IAM user.

Response Parameters

Table 5-240 Parameters in the response body

Parameter	Type	Description
user	Object	IAM user information.

Table 5-241 user

Parameter	Type	Description
enabled	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.

Parameter	Type	Description
id	String	IAM user ID.
domain_id	String	ID of the account to which the IAM user belongs.
name	String	IAM user name.
links	Object	IAM user resource link information.
password_expires_at	String	Password expiration time. If this parameter is set to **null**, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description	String	Description of the IAM user.

Table 5-242 user.links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for an administrator to create an IAM user named **IAMUser**

```
POST https://iam.myhuaweicloud.eu/v3/users
{
    "user": {
        "name": "IAMUser",
        "domain_id": "d78cbac186b744899480f25bd02...",
        "enabled": true,
        "password": "IAMPassword@",
        "description": "IAMDescription"
    }
}
```

Example Response

Status code: 201

The IAM user is created successfully.

```
{
    "user": {
        "description": "IAMDescription",
        "name": "IAMUser",
        "enabled": true,
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/users/076598a17b0010e21fdec003f3a2aa45"
        },
        "domain_id": "d78cbac186b744899480f25b...",
```

```
        "id": "076598a17b0010e21fdec003f3a2a..."
    }
}
```

Status Codes

Status Code	Description
201	The IAM user is created successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
409	A resource conflict occurs.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

For details, see **Error Codes**.

5.6.8 Changing the Login Password

Function

This API can be used by an IAM user to change the login password.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3/users/{user_id}/password

Table 5-243 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-244 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Token (no special permission requirements) of the IAM user corresponding to the **user_id** specified in the URL.

Table 5-245 Parameters in the request body

Parameter	Mandatory	Type	Description
user	Yes	Object	IAM user information.

Table 5-246 user

Parameter	Mandatory	Type	Description
password	Yes	String	New password, which must meet the following requirements: • Can contain 6 to 32 characters. The default minimum password length is 6 characters. • Must contain at least two of the following character types: uppercase letters, lowercase letters, digits, and special characters. • Cannot contain the user's mobile phone number or email address. • Must meet the password requirements defined in the account's **password policy**. • Must be different from the old password.
original_password	Yes	String	Old password of the IAM user.

Response Parameters

None

Example Request

Request for changing the login password from **IAMOriginalPassword@** to **IAMNewPassword@** as an IAM user

```
POST https://iam.myhuaweicloud.eu/v3/users/{user_id}/password
{
    "user": {
        "password": "IAMNewPassword@",
        "original_password": "IAMOriginalPassword@"
    }
}
```

Example Response

None

Status Codes

Status Code	Description
204	The password is changed successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.6.9 Modifying IAM User Information (Recommended)

Function

This API can be used by an IAM user to modify its basic information.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-USER/users/{user_id}/info

Table 5-247 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-248 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Token (no special permission requirements) of the IAM user corresponding to the **user_id** specified in the URL.

Table 5-249 Parameters in the request body

Parameter	Mandatory	Type	Description
user	Yes	Object	IAM user information.

Table 5-250 user

Parameter	Mandatory	Type	Description
email	No	String	Email address, which can contain not more than 255 characters.
mobile	No	String	Country code and new mobile number. The mobile number can contain not more than 32 digits.

Response Parameters

None

Example Request

Assume that an IAM user changes their email address to **IAMEmail@huawei.com** and the mobile number to .

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-USER/users/{user_id}/info
{
    "user": {
        "email": "IAMEmail@huawei.com",
        "mobile": ""
    }
}
```

Example Response

None

Status Codes

Status Code	Description
204	The user information is modified successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
409	A resource conflict occurs.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

For details, see **Error Codes**.

5.6.10 Modifying IAM User Information (Recommended)

Function

This API is provided for the **administrator** to modify IAM user information.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-USER/users/{user_id}

Table 5-251 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-252 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Token with **Security Administrator** permissions.

Table 5-253 Parameters in the request body

Parameter	Mandatory	Type	Description
user	Yes	Object	IAM user information.

Table 5-254 user

Parameter	Mandatory	Type	Description
name	No	String	New IAM user name, which consists of 1 to 32 characters. It can contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.) and cannot start with a digit or space.

Parameter	Mandatory	Type	Description
password	No	String	Password of the user. The password must meet the following requirements: • Can contain 6 to 32 characters. The default minimum password length is 6 characters. • Must contain at least two of the following character types: uppercase letters, lowercase letters, digits, and special characters. • Must meet the password requirements defined in the **password policy**. • Must be different from the old password.
email	No	String	Email address, which can contain not more than 255 characters.
areacode	No	String	Country code. The country code must be used together with a mobile number.
phone	No	String	New mobile number, which can contain a maximum of 32 digits. The mobile number must be used together with a country code.
enabled	No	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
pwd_status	No	Boolean	Password status. **true** means that the password needs to be changed, and **false** means that the password is normal.

Parameter	Mandatory	Type	Description
xuser_type	No	String	Type of the IAM user in the external system. The user type can contain a maximum of 64 characters. **xuser_type** must be used together with **xuser_id** and will be verified based on **xaccount_type** and **xdomain_type** of the same account. **NOTE** An external system refers to an enterprise management system connected to Huawei Cloud. Parameters **xaccount_type**, **xaccount_id**, **xdomain_type**, **xdomain_id**, **xuser_type**, and **xuser_id** cannot be obtained from Huawei Cloud. Please contact your enterprise administrator.
xuser_id	No	String	ID of the IAM user in the external system. The user ID can contain a maximum of 128 characters, and must be used together with **xuser_type**. Due to the latency, the IAM console may not be able to display the external identity ID you have set in real time. Refresh the page later. **NOTE** An external system refers to an enterprise management system connected to Huawei Cloud. Parameters **xaccount_type**, **xaccount_id**, **xdomain_type**, **xdomain_id**, **xuser_type**, and **xuser_id** cannot be obtained from Huawei Cloud. Please contact your enterprise administrator.
access_mode	No	String	Access type of the IAM user. • **default**: programmatic access and management console access. This option is the default access type. • **programmatic**: programmatic access • **console**: management console access
description	No	String	Description of the IAM user.

Response Parameters

Table 5-255 Parameters in the response body

Parameter	Type	Description
user	Object	IAM user information.

Table 5-256 user

Parameter	Type	Description
pwd_status	Boolean	Password status. **true** means that the password needs to be changed, and **false** means that the password is normal.
xuser_id	String	ID of the IAM user in the external system. **NOTE** An external system refers to an enterprise management system connected to Huawei Cloud. Parameters **xaccount_type**, **xaccount_id**, **xdomain_type**, **xdomain_id**, **xuser_type**, and **xuser_id** cannot be obtained from Huawei Cloud. Please contact your enterprise administrator.
xuser_type	String	Type of the IAM user in the external system. **NOTE** An external system refers to an enterprise management system connected to Huawei Cloud. Parameters **xaccount_type**, **xaccount_id**, **xdomain_type**, **xdomain_id**, **xuser_type**, and **xuser_id** cannot be obtained from Huawei Cloud. Please contact your enterprise administrator.
access_mode	String	Access type of the IAM user. • **default**: programmatic access and management console access. This option is the default access type. • **programmatic**: programmatic access • **console**: management console access
description	String	Description of the IAM user.
name	String	New IAM user name, which consists of 1 to 32 characters. It can contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.) and cannot start with a digit or space.
phone	String	New mobile number, which can contain a maximum of 32 digits. The mobile number must be used together with a country code.
domain_id	String	ID of the account to which the IAM user belongs.

Parameter	Type	Description
enabled	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
areacode	String	Country code.
email	String	New email address.
id	String	IAM user ID.
links	Object	IAM user resource link information.
password_expires_at	String	Password expiration time. This parameter will not be returned if its value is **null**. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Table 5-257 user.links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for an administrator to modify information of an IAM user named **IAMUser**: change the email address to **IAMEmail@huawei.com**, the mobile number to **12345678910**, and the password to **IAMPassword@**

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-USER/users/{user_id}
{
    "user": {
        "email": "IAMEmail@huawei.com",
        "areacode": "",
        "phone": "12345678910",
        "enabled": true,
        "name": "IAMUser",
        "password": "IAMPassword@",
        "pwd_status": false,
        "xuser_type": "",
        "xuser_id": "",
        "access_mode" : "default",
        "description": "IAMDescription"
    }
}
```

Example Response

Status code: 200

The request is successful.

```
{
    "user": {
        "description": "IAMDescription",
        "areacode": "",
        "enabled": true,
        "pwd_status": false,
        "xuser_id": "",
        "access_mode" : "default",
        "domain_id": "d78cbac186b744899480f25bd0...",
        "phone": "12345678910",
        "name": "IAMUser",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/3.0/OS-USER/users/076934ff9f0010cd1f0bc003..."
        },
        "id": "076934ff9f0010cd1f0bc0031019...",
        "xuser_type": "",
        "email": "IAMEmail@huawei.com"
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
409	A resource conflict occurs.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

For details, see **Error Codes**.

5.6.11 Modifying User Information

Function

This API is provided for the **administrator** to modify IAM user information.

The API can be called using both the global endpoint and region-specific endpoints.

Restrictions

This API cannot be used to change the mobile number and email address of an IAM user. To change the mobile number and email address, use the API described in **Modifying IAM User Information (Recommended)**.

URI

PATCH /v3/users/{user_id}

Table 5-258 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-259 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-260 Parameters in the request body

Parameter	Mandatory	Type	Description
user	Yes	Object	IAM user information.

Table 5-261 user

Parameter	Mandatory	Type	Description
domain_id	No	String	ID of the account to which the IAM user belongs.
name	No	String	New IAM user name, which consists of 1 to 32 characters. It can contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.) and cannot start with a digit or space.
password	No	String	New password, which must meet the following requirements: • Can contain 6 to 32 characters. The default minimum password length is 6 characters. • Must contain at least two of the following character types: uppercase letters, lowercase letters, digits, and special characters. • Cannot contain the user's mobile phone number or email address. • Must meet the password requirements defined in the **password policy**. • Must be different from the old password.
enabled	No	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
description	No	String	Description of the IAM user.
pwd_status	No	Boolean	Password status. **true** means that the password needs to be changed, and **false** means that the password is normal.

Response Parameters

Table 5-262 Parameters in the response body

Parameter	Type	Description
user	Object	IAM user information.

Table 5-263 user

Parameter	Type	Description
name	String	IAM user name.
domain_id	String	ID of the account to which the IAM user belongs.
enabled	Boolean	Enabling status of the IAM user. **true** (default value) indicates that the user is enabled. **false** indicates that the user is disabled.
id	String	IAM user ID.
password_expires_at	String	Password expiration time. If this parameter is set to **null**, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description	String	Description of the IAM user.
pwd_status	Boolean	Password status. **true** means that the password needs to be changed, and **false** means that the password is normal.
last_project_id	String	ID of the project that the IAM user lastly accessed before exiting the system.
extra	Object	Other information about the IAM user.
links	Object	IAM user resource link information.

Table 5-264 user.extra

Parameter	Type	Description
description	String	Description of the IAM user.
pwd_status	Boolean	Password status. **true** means that the password needs to be changed, and **false** means that the password is normal.
last_project_id	String	ID of the project that the IAM user lastly accessed before exiting the system.

Table 5-265 user.links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for an administrator to change the password of IAM user named **IAMUser** to **IAMPassword@**

```
PATCH https://iam.myhuaweicloud.eu/v3/users/{user_id}
{
    "user": {
        "domain_id": "d78cbac186b744899480f25bd02...",
        "name": "IAMUser",
        "password": "IAMPassword@",
        "enabled": true,
        "pwd_status": false,
        "description": "IAMDescription"
    }
}
```

Example Response

Status code: 200

The request is successful.

```
{
    "user": {
        "pwd_status": false,
        "description": "IAMDescription",
        "name": "IAMUser",
        "extra": {
            "pwd_status": false,
            "description": "IAMDescription",
        },
        "enabled": true,
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/users/07609fb9358010e21f7bc003751c7..."
        },
        "id": "07609fb9358010e21f7bc003751c7...",
        "domain_id": "d78cbac186b744899480f25bd02..."
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
409	A resource conflict occurs.

Status Code	Description
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

For details, see **Error Codes**.

5.6.12 Deleting an IAM User

Function

This API is provided for the **administrator** to delete an IAM user.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3/users/{user_id}

Table 5-266 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-267 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for deleting an IAM user

```
DELETE https://iam.myhuaweicloud.eu/v3/users/{user_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The IAM user is deleted successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

For details, see **Error Codes**.

5.7 User Group Management

5.7.1 Listing User Groups

Function

This API is provided for the **administrator** to list all user groups.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/groups

Table 5-268 Query parameters

Parameter	Mandatory	Type	Description
domain_id	No	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
name	No	String	User group name, which can contain a maximum of 64 characters. For details about how to obtain a user group name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-269 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-270 Parameters in the response body

Parameter	Type	Description
groups	Array of objects	User group information.
links	Object	Resource link information.

Table 5-271 groups

Parameter	Type	Description
description	String	User group description.
id	String	User group ID.
domain_id	String	ID of the account to which the user group belongs.
name	String	User group name.
links	Object	User group resource link.
create_time	Long	Time when the user group was created.

Table 5-272 groups.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-273 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying a list of user groups

```
GET https://iam.myhuaweicloud.eu/v3/groups
```

Example Response

Status code: 200

The request is successful.

```
{
   "groups": [
      {
         "domain_id": "d78cbac186b744899480f25bd02...",
         "create_time": 1536293929624,
         "name": "IAMGroupA",
         "description": "IAMDescription",
         "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/groups/5b050baea9db472c88cbae67..."
         },
         "id": "5b050baea9db472c88cbae6..."
      },
      {
         "domain_id": "d78cbac186b744899480f25...",
         "create_time": 1578107542861,
         "name": "IAMGroupB",
         "description": "IAMDescription",
         "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/groups/07609e7eb200250a3f7dc003cb7a4e2d"
         },
         "id": "07609e7eb200250a3f7dc003cb..."
      }
   ],
   "links": {
      "next": null,
      "previous": null,
      "self": "https://iam.myhuaweicloud.eu/v3/groups"
   }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.

Error Codes

None

5.7.2 Querying User Group Details

Function

This API is provided for the **administrator** to query user group information.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/groups/{group_id}

Table 5-274 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-275 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-276 Parameters in the response body

Parameter	Type	Description
group	Object	User group information.

Table 5-277 group

Parameter	Type	Description
description	String	User group description.
id	String	User group ID.
domain_id	String	ID of the account to which the user group belongs.
name	String	User group name.
links	Object	User group resource link.
create_time	Long	Time when the user group was created.

Table 5-278 group.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying user group details

```
GET https://iam.myhuaweicloud.eu/v3/groups/{group_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "group": {
        "domain_id": "d78cbac186b744899480f25bd02...",
        "create_time": 1578107542861,
        "name": "IAMGroup",
        "description": "",
        "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/groups/07609e7eb200250a3f7dc003cb7a..."
        },
        "id": "07609e7eb200250a3f7dc003cb7..."
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Error Codes

None

5.7.3 Creating a User Group

Function

This API is provided for the **administrator** to create a user group.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3/groups

Request Parameters

Table 5-279 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-280 Parameters in the request body

Parameter	Mandatory	Type	Description
group	Yes	Object	User group information.

Table 5-281 group

Parameter	Mandatory	Type	Description
description	No	String	User group description, which must contain less than or equal to 255 characters.
domain_id	No	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
name	Yes	String	User group name, which must contain less than or equal to 64 characters.

Response Parameters

Table 5-282 Parameters in the response body

Parameter	Type	Description
group	Object	User group information.

Table 5-283 group

Parameter	Type	Description
description	String	User group description.
id	String	User group ID.
domain_id	String	ID of the account to which the user group belongs.
name	String	User group name.
links	Object	User group resource link.
create_time	Long	Time when the user group was created.

Table 5-284 group.links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for an administrator to create a user group named **IAMGroup**

```
POST https://iam.myhuaweicloud.eu/v3/groups
{
    "group": {
        "description": "IAMDescription",
        "domain_id": "d78cbac186b744899480f25bd0...",
        "name": "IAMGroup"
    }
}
```

Example Response

Status code: 201

The user group is created successfully.

```
{
    "group": {
        "description": "IAMDescription",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/groups/077a4c7bcd8010d53fb7c003e9d966c2"
        },
        "id": "077a4c7bcd8010d53fb7c003e9d966c2",
        "create_time": 1578969208707,
        "domain_id": "d78cbac186b744899480f25bd0...",
        "name": "IAMGroup"
    }
}
```

Status Codes

Status Code	Description
201	The user group is created successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
409	A resource conflict occurs.

Error Codes

None

5.7.4 Updating User Group Information

Function

This API is provided for the **administrator** to update user group information.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PATCH /v3/groups/{group_id}

Table 5-285 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-286 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-287 Parameters in the request body

Parameter	Mandatory	Type	Description
group	Yes	Object	User group information.

Table 5-288 group

Parameter	Mandatory	Type	Description
description	No	String	User group description, which must contain less than or equal to 255 characters. Either **name** or **description** must be specified.
domain_id	No	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
name	No	String	User group name, which must contain less than or equal to 64 characters. Either **name** or **description** must be specified.

Response Parameters

Table 5-289 Parameters in the response body

Parameter	Type	Description
group	Object	User group information.

Table 5-290 group

Parameter	Type	Description
description	String	User group description.
id	String	User group ID.
domain_id	String	ID of the account to which the user group belongs.
name	String	User group name.
links	Object	User group resource link.
create_time	Long	Time when the user group was created.

Table 5-291 group.links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for changing the user group name to **IAMGroup** and description to **IAMDescription**

```
PATCH https://iam.myhuaweicloud.eu/v3/groups/{group_id}
{
    "group": {
        "description": "IAMDescription",
        "domain_id": "d78cbac186b744899480f25bd02...",
        "name": "IAMGroup"
    }
}
```

Example Response

Status code: 200

The request is successful.

```
{
    "group": {
        "description": "IAMDescription",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/groups/077a4da48a00251f3f9dc0032103400f"
        },
        "id": "077a4da48a00251f3f9dc0032103400f",
        "create_time": 1578969360636,
        "domain_id": "d78cbac186b744899480f25bd...",
        "name": "IAMGroup"
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
409	A resource conflict occurs.
501	The API is not available.

Error Codes

None

5.7.5 Deleting a User Group

Function

This API is provided for the **administrator** to delete a user group.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3/groups/{group_id}

Table 5-292 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-293 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for deleting a user group

```
DELETE https://iam.myhuaweicloud.eu/v3/groups/{group_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The user group is deleted successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Error Codes

None

5.7.6 Checking Whether an IAM User Belongs to a User Group

Function

This API is provided for the **administrator** to check whether an IAM user belongs to a specified user group.

The API can be called using both the global endpoint and region-specific endpoints.

URI

HEAD /v3/groups/{group_id}/users/{user_id}

Table 5-294 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-295 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for checking whether an IAM user belongs to a user group

```
HEAD https://iam.myhuaweicloud.eu/v3/groups/{group_id}/users/{user_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The request is successful. (The IAM user belongs to the user group.)
400	Invalid parameters.
401	Authentication failed.
403	Access denied.

Status Code	Description
404	The requested resource cannot be found. (The IAM user does not belong to the user group.)

Error Codes

None

5.7.7 Adding an IAM User to a User Group

Function

This API is provided for the **administrator** to add an IAM user to a specified user group.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3/groups/{group_id}/users/{user_id}

Table 5-296 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-297 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for adding an IAM user to a user group

```
PUT https://iam.myhuaweicloud.eu/v3/groups/{group_id}/users/{user_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The IAM user is successfully added to the user group.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Error Codes

None

5.7.8 Removing an IAM User from a User Group

Function

This API can be used by the **administrator** to remove an IAM user from a specified user group.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3/groups/{group_id}/users/{user_id}

Table 5-298 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-299 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for removing an IAM user from a user group

```
DELETE https://iam.myhuaweicloud.eu/v3/groups/{group_id}/users/{user_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The IAM user is successfully removed from the user group.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found. (The IAM user does not belong to the user group.)

Error Codes

None

5.8 Permissions Management

5.8.1 Listing Permissions

Function

This API is provided for the **administrator** to list all permissions.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/roles

Table 5-300 Query parameters

Parameter	Mandatory	Type	Description
domain_id	No	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. **NOTE** • If this parameter is specified, only custom policies of the account will be returned. • If this parameter is not specified, all system permissions (including system-defined policies and roles) will be returned.

Parameter	Mandatory	Type	Description
permission_type	No	String	System permission type. This parameter is valid only when **domain_id** is left blank. • **policy**: system-defined policy • **role**: system-defined role
name	No	String	Permission name for internal use. For example, **ccs_user** is the internal name of the **CCS User** role for Cloud Catalog Service (CCS). **It is recommended that the display_name parameter rather than the name parameter be transferred.**
display_name	No	String	Permission name or filter condition. The value of this parameter can be the permission name displayed on the console or included in **System Permissions**. • Permission name: For example, if you set this parameter to **ECS FullAccess**, information about the permission will be returned. • Filter condition: For example, if you set this parameter to **Administrator**, all administrator permissions that meet the conditions will be returned.
page	No	Integer	Page number for pagination query, which must be used together with **per_page**. The minimum value is **1**. You can use this parameter when you set **domain_id** to query custom policies.
per_page	No	Integer	Number of data records to be displayed on each page. The value ranges from 1 to 300, and the default value is **300**. This parameter must be used together with **page**. A maximum of 300 permissions will be displayed on each page if the **page** and **per_page** parameters are not transferred.

Parameter	Mandatory	Type	Description
type	No	String	Display mode of the permission. The options include **domain**, **project**, and **all**. **domain** means returning all permissions of the AA and AX levels; **project** means returning all permissions of the AA and XA levels; **all** means returning permissions of the AA, AX, and XA permissions. **NOTE** • **AX**: Account level. • **XA**: Project level. • **AA**: Both the account level and project level. • **XX**: Neither the account level nor project level.
catalog	No	String	Service catalog, which corresponds to the **catalog** field in policies. You can set this parameter to query system-defined policies and custom policies.

Request Parameters

Table 5-301 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-302 Parameters in the response body

Parameter	Type	Description
links	Object	Resource link information.
roles	Array of objects	Permission information.

Parameter	Type	Description
total_number	Integer	Total number of permissions.

Table 5-303 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-304 roles

Parameter	Type	Description
domain_id	String	ID of the account to which the permission belongs.
flag	String	If this parameter is set to **fine_grained**, the permission is a system-defined policy.
description_cn	String	Description of the permission in Chinese.
catalog	String	Service catalog of the permission.
name	String	Permission name for internal use. For example, **ccs_user** is the internal name of the **CCS User** role for CCS. This parameter is carried in the token of a user, allowing the system to determine whether the user has permissions to access a specific cloud service.
description	String	Description of the permission.
links	Object	Permission resource link.
id	String	Permission ID.
display_name	String	Permission name.

Parameter	Type	Description
type	String	Display mode of the permission. **NOTE** • **AX**: Account level. • **XA**: Project level. • **AA**: Both the account level and project level. • **XX**: Neither the account level nor project level. • The display mode of a custom policy can only be **AX** or **XA**. A custom policy must be displayed at either of the two levels.
policy	Object	Content of the permission.
updated_time	String	Time when the permission was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.
created_time	String	Time when the permission was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.

Table 5-305 roles.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-306 roles.policy

Parameter	Type	Description
Depends	Array of objects	Dependent permissions.
Statement	Array of objects	Statement of the permission.

Parameter	Type	Description
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.

Table 5-307 roles.policy.Depends

Parameter	Type	Description
catalog	String	Service catalog of the permission.
display_name	String	Display name of the permission.

Table 5-308 roles.policy.Statement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Parameter	Type	Description
Condition	Object	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**. **NOTE** Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**). `"Condition": { "StringEquals": { "obs:prefix": [ "public" ] } }`
Resource	Array of strings	Cloud resource. **NOTE** • Format: *:::::*. For example, **obs:::bucket:***. Asterisks are allowed. • The region segment can be * or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Table 5-309 roles.policy.Statement.Condition.operator

Parameter	Type	Description
attribute	Array of strings	Condition key. The condition key must correspond to the specified operator. A maximum of 10 condition keys are allowed. The parameter type is custom character string array.

Example Request

Request for querying permissions

```
GET https://iam.myhuaweicloud.eu/v3/roles
```

Example Response

Status code: 200

The request is successful.

```
{
  "roles" : [ {
    "domain_id" : null,
```

```
    "description_cn" : "Description of the permission in Chinese",
    "catalog" : "VulnScan",
    "name" : "wscn_adm",
    "description" : "Vulnerability Scan Service administrator of tasks and reports.",
    "links" : {
      "next" : null,
      "previous" : null,
      "self" : "https://iam.myhuaweicloud.eu/v3/roles/0af84c1502f447fa9c2fa18083fbb87e"
    },
    "id" : "0af84c1502f447fa9c2fa18083fbb87e",
    "display_name" : "VSS Administrator",
    "type" : "XA",
    "policy" : {
      "Version" : "1.0",
      "Statement" : [ {
        "Action" : [ "WebScan:*:*" ],
        "Effect" : "Allow"
      } ],
      "Depends" : [ {
        "catalog" : "BASE",
        "display_name" : "Server Administrator"
      }, {
        "catalog" : "BASE",
        "display_name" : "Tenant Guest"
      } ]
    }
  }, {
    "domain_id" : null,
    "flag" : "fine_grained",
    "description_cn" : "Description of the permission in Chinese",
    "catalog" : "CSE",
    "name" : "system_all_34",
    "description" : "All permissions of CSE service.",
    "links" : {
      "next" : null,
      "previous" : null,
      "self" : "https://iam.myhuaweicloud.eu/v3/roles/0b5ea44ebdc64a24a9c372b2317f7e39"
    },
    "id" : "0b5ea44ebdc64a24a9c372b2317f7e39",
    "display_name" : "CSE Admin",
    "type" : "XA",
    "policy" : {
      "Version" : "1.1",
      "Statement" : [ {
        "Action" : [ "cse:*:*", "ecs:*:*", "evs:*:*", "vpc:*:*" ],
        "Effect" : "Allow"
      } ]
    }
  } ],
  "links" : {
    "next" : null,
    "previous" : null,
    "self" : "https://iam.myhuaweicloud.eu/v3/roles"
  },
  "total_number" : 300
}
```


Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.

Status Code	Description
403	Access denied.

Error Codes

None

5.8.2 Querying Permission Details

Function

This API is provided for the **administrator** to query permission details.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/roles/{role_id}

Table 5-310 URI parameters

Parameter	Mandatory	Type	Description
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-311 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-312 Parameters in the response body

Parameter	Type	Description
role	Object	Permission information.

Table 5-313 role

Parameter	Type	Description
domain_id	String	ID of the account to which the permission belongs.
flag	String	If this parameter is set to **fine_grained**, the permission is a system-defined policy.
description_cn	String	Description of the permission in Chinese.
catalog	String	Service catalog of the permission.
name	String	Permission name for internal use. For example, **ccs_user** is the internal name of the **CCS User** role for CCS. This parameter is carried in the token of a user, allowing the system to determine whether the user has permissions to access a specific cloud service.
description	String	Description of the permission.
links	Object	Permission resource link.
id	String	Permission ID.
display_name	String	Permission name.
type	String	Display mode of the permission. **NOTE** • **AX**: Account level. • **XA**: Project level. • **AA**: Both the account level and project level. • **XX**: Neither the account level nor project level. • The display mode of a custom policy can only be **AX** or **XA**. A custom policy must be displayed at either of the two levels.
policy	Object	Content of the permission.

Parameter	Type	Description
updated_time	String	Time when the permission was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
created_time	String	Time when the permission was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Table 5-314 role.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-315 role.policy

Parameter	Type	Description
Depends	Array of objects	Dependent permissions.
Statement	Array of objects	Statement of the permission.
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.

Table 5-316 role.policy.Depends

Parameter	Type	Description
catalog	String	Service catalog of the permission.

Parameter	Type	Description
display_name	String	Display name of the permission.

Table 5-317 role.policy.Statement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Condition	Object	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**.
		NOTE
		Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**).
		`"Condition": {`
		`"StringEquals": {`
		`"obs:prefix": [`
		`"public"`
		`]`
		`}`
		`}`

Parameter	Type	Description
Resource	Array of strings	Cloud resource. **NOTE** • Format: *:::::*. For example, **obs:::bucket:***. Asterisks are allowed. • The region segment can be ***** or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Example Request

Request for querying permission details

```
GET https://iam.myhuaweicloud.eu/v3/roles/{role_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "role": {
        "domain_id": null,
        "description_cn": "Description of the permission in Chinese",
        "catalog": "VulnScan",
        "name": "wscn_adm",
        "description": "Vulnerability Scan Service administrator of tasks and reports.",
        "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/roles/0af84c1502f447fa9c2fa18083fbb87e"
        },
        "id": "0af84c1502f447fa9c2fa18083fbb87e",
        "display_name": "VSS Administrator",
        "type": "XA",
        "policy": {
            "Version": "1.0",
            "Statement": [
                {
                    "Action": [
                        "WebScan:*:*"
                    ],
                    "Effect": "Allow"
                }
            ],
            "Depends": [
                {
                    "catalog": "BASE",
                    "display_name": "Server Administrator"
                },
                {
                    "catalog": "BASE",
                    "display_name": "Tenant Guest"
                }
```



```
        ]
      }
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Error Codes

None

5.8.3 Querying Permissions Assignment Records

Function

This API is used to query permissions assignment records of a specified account.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-PERMISSION/role-assignments

Table 5-318 Query parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	No	String	Policy ID.
subject	No	String	Principal. The value can be **user**, **group**, or **agency**. This parameter is exclusive with **subject.user_id**, **subject.group_id**, and **subject.agency_id**.

Parameter	Mandatory	Type	Description
subject.user_id	No	String	ID of the IAM user. For details about how to obtain the ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
subject.group_id	No	String	ID of the user group. For details about how to obtain the ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
subject.agency_id	No	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
scope	No	String	Authorization scope. The value can be **project**, **domain**, or **enterprise_project**. This parameter is mutually exclusive with **scope.project_id**, **scope.domain_id**, and **scope.enterprise_projects_id**. **NOTE** • To view global service authorization records, set this parameter to **domain** or specify **scope.domain_id**. • To view resource-based authorization records, set this parameter to **domain** and **is_inherited** to **true**. • To view project-based authorization records, set this parameter to **project** or specify **scope.project_id**. • To view enterprise project-based authorization records, set this parameter to **enterprise_project** or specify **scope.enterprise_project_id**.
scope.project_id	No	String	Project ID. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
scope.domain_id	No	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
scope.enterprise_projects_id	No	String	ID of the authorized enterprise project. For details about how to obtain the ID, see **How Do I Obtain an Enterprise Project ID?**

Parameter	Mandatory	Type	Description
is_inherited	No	Boolean	Whether to include all project-based authorization records. The default value is **false**. This parameter is valid only when **scope** is set to **domain** or **scope.domain_id** is specified. **true**: Query all project-based authorization records. **false**: Query global service authorization records.
include_group	No	Boolean	Whether to include user group-based authorization records. The default value is **true**. This parameter is valid only when **subject** is set to **user** or **subject.user_id** is specified. **true**: Query authorization records of IAM users and user groups to which the IAM users belong. **false**: Only query authorization records of IAM users.
page	No	String	Page number for pagination query. The minimum value is **1**. This parameter must be used together with **per_page**.
per_page	No	String	Number of data records to be displayed on each page during pagination query. The value ranges from 1 to 50. This parameter must be specified together with **page**.

Request Parameters

Table 5-319 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access credential issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Permissions Management**.

Response Parameters

Table 5-320 Parameters in the response body

Parameter	Type	Description
total_num	Long	Total number of returned authorization records.
role_assignments	Array of RoleAssignmentBody objects	Authorization information.

Table 5-321 role_assignments

Parameter	Type	Description
user	RoleUserAssignmentId object	Authorized user.
role	RoleAssignmentId object	Authorization policy.
group	RoleGroupAssignmentId object	Authorized user group.
agency	RoleAgencyAssignmentId object	Authorization agency.
scope	RoleAssignmentScope object	Authorization scope.
is_inherited	Boolean	Whether the authorization is based on all projects.

Table 5-322 role_assignments.user

Parameter	Type	Description
id	String	IAM user ID.

Table 5-323 role_assignments.role

Parameter	Type	Description
id	String	Permission ID.

Table 5-324 role_assignments.group

Parameter	Type	Description
id	String	User group ID.

Table 5-325 role_assignments.agency

Parameter	Type	Description
id	String	Agency ID.

Table 5-326 role_assignments.scope

Parameter	Type	Description
project	RoleProjectAssignmentId object	IAM project-based authorization.
domain	RoleDomainAssignmentId object	Authorization based on global services or all projects.
enterprise_project	RoleEnterpriseProjectAssignmentId object	Enterprise project-based authorization.

Table 5-327 role_assignments.scope.project

Parameter	Type	Description
id	String	IAM project ID.

Table 5-328 role_assignments.scope.domain

Parameter	Type	Description
id	String	Global service ID.

Table 5-329 role_assignments.scope.enterprise_project

Parameter	Type	Description
id	String	Enterprise project ID.

Example Request

Request for querying permissions assignment records

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/role-assignments?{domain_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "role_assignments":{
        "group":{
            "id":"07609e7eb200250a3f7dc003cb7a4e2d"
        },
        "is_inherited":true,
        "role":{
            "id":"11e5c42d20cc349a2b9e2f8afd253f50c"
        },
        "scope":{
            "domain":{
                "id":"d78cbac186b744899480f25bd022f468"
            }
        }
    },
    "total_num":1
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.

Error Codes

For details, see **Error Codes**.

5.8.4 Querying Permissions of a User Group for a Global Service Project

Function

This API is provided for the **administrator** to query the permissions of a user group for a global service project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/domains/{domain_id}/groups/{group_id}/roles

Table 5-330 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-331 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-332 Parameters in the response body

Parameter	Type	Description
links	Object	Resource link information.
roles	Array of objects	Permission information.

Table 5-333 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-334 roles

Parameter	Type	Description
domain_id	String	ID of the account to which the permission belongs.
flag	String	If this parameter is set to **fine_grained**, the permission is a system-defined policy.
description_cn	String	Description of the permission in Chinese.
catalog	String	Service catalog of the permission.
name	String	Permission name for internal use. For example, **ccs_user** is the internal name of the **CCS User** role for CCS. This parameter is carried in the token of a user, allowing the system to determine whether the user has permissions to access a specific cloud service.
description	String	Description of the permission.
links	Object	Permission resource link.
id	String	Permission ID.
display_name	String	Permission name.
type	String	Display mode of the permission. **NOTE** • **AX**: Account level. • **XA**: Project level. • **AA**: Both the account level and project level. • **XX**: Neither the account level nor project level. • The display mode of a custom policy can only be **AX** or **XA**. A custom policy must be displayed at either of the two levels.
policy	Object	Content of the permission.

Parameter	Type	Description
updated_time	String	Time when the permission was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
created_time	String	Time when the permission was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Table 5-335 roles.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-336 roles.policy

Parameter	Type	Description
Depends	Array of objects	Dependent permissions.
Statement	Array of objects	Statement of the permission.
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.

Table 5-337 roles.policy.Depends

Parameter	Type	Description
catalog	String	Service catalog of the permission.

Parameter	Type	Description
display_name	String	Display name of the permission.

Table 5-338 roles.policy.Statement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Condition	Object	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**.
		NOTE
		Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**).
		`"Condition": {`
		`"StringEquals": {`
		`"obs:prefix": [`
		`"public"`
		`]`
		`}`
		`}`

Parameter	Type	Description
Resource	Array of strings	Cloud resource. **NOTE** • Format: *:::::*. For example, **obs:*:*bucket:***. Asterisks are allowed. • The region segment can be ***** or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Example Request

Request for querying the permissions of a user group for a global service project

```
GET https://iam.myhuaweicloud.eu/v3/domains/{domain_id}/groups/{group_id}/roles
```

Example Response

Status code: 200

The request is successful.


```
{
   "roles": [
      {
         "domain_id": null,
         "flag": "fine_grained",
         "description_cn": "Description of the permission in Chinese",
         "catalog": "CDN",
         "name": "system_all_11",
         "description": "Allow Query Domains",
         "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/roles/db4259cce0ce47c9903dfdc195eb453b"
         },
         "id": "db4259cce0ce47c9903dfdc195eb453b",
         "display_name": "CDN Domain Viewer",
         "type": "AX",
         "policy": {
            "Version": "1.1",
            "Statement": [
               {
                  "Action": [
                     "cdn:configuration:queryDomains",
                     "cdn:configuration:queryOriginServerInfo",
                     "cdn:configuration:queryOriginConfInfo",
                     "cdn:configuration:queryHttpsConf",
                     "cdn:configuration:queryCacheRule",
                     "cdn:configuration:queryReferConf",
                     "cdn:configuration:queryChargeMode",
                     "cdn:configuration:queryCacheHistoryTask",
                     "cdn:configuration:queryIpAcl",
                     "cdn:configuration:queryResponseHeaderList"
                  ],
                  "Effect": "Allow"
```



```
                }
            ]
        }
    }
  ],
  "links": {
    "next": null,
    "previous": null,
    "self": "https://iam.myhuaweicloud.eu/v3/domains/d78cbac186b744899480f25bd022f468/groups/
077d71374b8025173f61c003ea0a11ac/roles"
  }
}
```


Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Error Codes

None

5.8.5 Querying Permissions of a User Group for a Region-specific Project

Function

This API is provided for the **administrator** to query the permissions of a user group for a region-specific project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/projects/{project_id}/groups/{group_id}/roles

Table 5-339 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
project_id	Yes	String	Project ID. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-340 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-341 Parameters in the response body

Parameter	Type	Description
links	Object	Resource link information.
roles	Array of objects	Permission information.

Table 5-342 links

Parameter	Type	Description
self	String	Resource link.

Parameter	Type	Description
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-343 roles

Parameter	Type	Description
domain_id	String	ID of the account to which the permission belongs.
flag	String	If this parameter is set to **fine_grained**, the permission is a system-defined policy.
description_cn	String	Description of the permission in Chinese.
catalog	String	Service catalog of the permission.
name	String	Permission name for internal use. For example, **ccs_user** is the internal name of the **CCS User** role for CCS. This parameter is carried in the token of a user, allowing the system to determine whether the user has permissions to access a specific cloud service.
description	String	Description of the permission.
links	Object	Permission resource link.
id	String	Permission ID.
display_name	String	Permission name.
type	String	Display mode of the permission. **NOTE** • **AX**: Account level. • **XA**: Project level. • **AA**: Both the account level and project level. • **XX**: Neither the account level nor project level. • The display mode of a custom policy can only be **AX** or **XA**. A custom policy must be displayed at either of the two levels.
policy	Object	Content of the permission.
updated_time	String	Time when the permission was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Parameter	Type	Description
created_time	String	Time when the permission was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Table 5-344 roles.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-345 roles.policy

Parameter	Type	Description
Depends	Array of objects	Dependent permissions.
Statement	Array of objects	Statement of the permission.
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.

Table 5-346 roles.policy.Depends

Parameter	Type	Description
catalog	String	Service catalog of the permission.
display_name	String	Permission name.

Table 5-347 roles.policy.Statement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Condition	Object	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**.
		NOTE
		Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**).
		`"Condition": {`
		`"StringEquals": {`
		`"obs:prefix": [`
		`"public"`
		`]`
		`}`
		`}`

Resource	Array of strings	Cloud resource. **NOTE** • Format: *:::::*. For example, **obs:*:bucket:***. Asterisks are allowed. • The region segment can be * or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Example Request

Request for querying the permissions of a user group for a region-specific project

```
GET https://iam.myhuaweicloud.eu/v3/projects/{project_id}/groups/{group_id}/roles
```

Example Response

Status code: 200

The request is successful.

```
{
   "roles": [
      {
         "domain_id": null,
         "flag": "fine_grained",
         "description_cn": "Description of the permission in Chinese",
         "catalog": "AOM",
         "name": "system_all_30",
         "description": "AOM read only",
         "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/roles/75cfe22af2b3498d82b655fbb39de498"
         },
         "id": "75cfe22af2b3498d82b655fbb39de498",
         "display_name": "AOM Viewer",
         "type": "XA",
         "policy": {
            "Version": "1.1",
            "Statement": [
               {
                  "Action": [
                     "aom:*:list",
                     "aom:*:get",
                     "apm:*:list",
                     "apm:*:get"
                  ],
                  "Effect": "Allow"
               }
            ]
         }
      }
   ],
   "links": {
      "next": null,
      "previous": null,
      "self": "https://iam.myhuaweicloud.eu/v3/projects/065a7c66da0010992ff7c0031e5a5e7d/groups/
077d71374b8025173f61c003ea0a11ac/roles"
   }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.

Status Code	Description
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Error Codes

None

5.8.6 Granting Permissions to a User Group for a Global Service Project

Function

This API is provided for the **administrator** to grant permissions to a user group for a global service project. For details about the authorization scope, see **System Permissions**.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}

Table 5-348 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Parameter	Mandatory	Type	Description
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**. **NOTE** To assign a custom policy that contains OBS operations to a user group, create two custom policies with the scope being set to global services and region-specific projects respectively and other parameters being the same, and then attach the two policies to the user group.

Request Parameters

Table 5-349 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for granting permissions to a user group for a global service project

```
PUT https://iam.myhuaweicloud.eu/v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The authorization is successful.

Status Code	Description
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
409	A resource conflict occurs.

Error Codes

None

5.8.7 Granting Permissions to a User Group for a Region-specific Project

Function

This API is provided for the **administrator** to grant permissions to a user group for a region-specific project. For details about the authorization scope, see **System Permissions**.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}

Table 5-350 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Parameter	Mandatory	Type	Description
project_id	Yes	String	ID of the project for which the user group will be assigned permissions. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. Ensure that the project is the IAM project that IAM users in the group will be authorized to access and use. **NOTE** To assign a custom policy that contains OBS operations to a user group, use the API described in **Querying Project Information** to obtain the ID of the **MOS** project, and attach the custom policy to the user group in this project.
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-351 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for granting permissions to a user group for a region-specific project

```
PUT https://iam.myhuaweicloud.eu/v3/projects/{project_id}/groups/{group_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The authorization is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
409	A resource conflict occurs.

Error Codes

None

5.8.8 Checking Whether a User Group Has Specified Permissions for a Global Service Project

Function

This API is provided for the **administrator** to check whether a user group has specified permissions for a global service project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}

Table 5-352 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-353 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for checking whether a user group has specified permissions for a global service project

```
HEAD https://iam.myhuaweicloud.eu/v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The request is successful. (The user group has the specified permissions for the global service project.)
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Error Codes

None

5.8.9 Checking Whether a User Group Has Specified Permissions for a Region-specific Project

Function

This API is provided for the **administrator** to check whether a user group has specified permissions for a region-specific project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}

Table 5-354 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
project_id	Yes	String	Project ID. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Parameter	Mandatory	Type	Description
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-355 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for checking whether a user group has specified permissions for a region-specific project

```
HEAD https://iam.myhuaweicloud.eu/v3/projects/{project_id}/groups/{group_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The request is successful. (The user group has the specified permissions for the region-specific project.)
400	Invalid parameters.
401	Authentication failed.
403	Access denied.

Status Code	Description
404	The requested resource cannot be found.

Error Codes

None

5.8.10 Querying All Permissions of a User Group

Function

This API is provided for the **administrator** to query all permissions that have been assigned to a user group.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/inherited_to_projects

Table 5-356 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-357 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token with **Security Administrator** permissions.

Response Parameters

Status code: 200

Table 5-358 Parameters in the response body

Parameter	Type	Description
links	object	Resource link information.
roles	Array of objects	Permission information.
total_number	Integer	Total number of custom policies. This parameter is returned only when **domain_id** is specified in the request.

Table 5-359 RoleResult

Parameter	Type	Description
domain_id	String	ID of the account to which the permission belongs.
flag	String	If this parameter is set to **fine_grained**, the permission is a system-defined policy.
description_cn	String	Description of the permission in Chinese.
catalog	String	Service catalog of the permission.
name	String	Permission name. This parameter is carried in the token of a user, allowing the system to determine whether the user has permissions to access a specific cloud service.
description	String	Description of the permission.
links	object	Permission resource link.
id	String	Permission ID.
display_name	String	Display name of the permission.

Parameter	Type	Description
type	String	Display mode of the permission. **NOTE** • **AX**: Account level. • **XA**: Project level. • **AA**: Both the account level and project level. • **XX**: Neither the account level nor project level. • The display mode of a custom policy can only be **AX** or **XA**. A custom policy must be displayed at either of the two levels.
policy	object	Content of the permission.
updated_time	String	Time when the permission was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
created_time	String	Time when the permission was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Table 5-360 Links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-361 RolePolicy

Parameter	Type	Description
Depends	Array of objects	Dependent permissions.
Statement	Array of objects	Statement of the permission.

Parameter	Type	Description
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.

Table 5-362 PolicyDepends

Parameter	Type	Description
catalog	String	Service catalog of the permission.
display_name	String	Display name of the permission.

Table 5-363 PolicyStatement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Enumerated values: • Allow • Deny

Parameter	Type	Description
Condition	Object	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**. **NOTE** Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**). `"Condition": { "StringEquals": { "obs:prefix": [ "public" ] } }`
Resource	Array of strings	Cloud resource. **NOTE** • Format: *:::::*. For example, **obs:::bucket:***. Asterisks are allowed. • The region segment can be ***** or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Example Request

Request for querying all permissions of a user group

```
GET https://iam.myhuaweicloud.eu/v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/inherited_to_projects
```

Example Response

Status code: 200

The request is successful.

```
{
  "roles" : [ {
    "domain_id" : null,
    "description_cn" : "Description of the permission in Chinese",
    "catalog" : "VulnScan",
    "name" : "wscn_adm",
    "description" : "Vulnerability Scan Service administrator of tasks and reports.",
    "links" : {
      "next" : null,
      "previous" : null,
      "self" : "https://iam.myhuaweicloud.eu/v3/roles/0af84c1502f447fa9c2fa18083fbb..."
    },
    "id" : "0af84c1502f447fa9c2fa18083fbb...",
    "display_name" : "VSS Administrator",
    "type" : "XA",
    "policy" : {
      "Version" : "1.0",
      "Statement" : [ {
```



```
      "Action" : [ "WebScan:*:*" ],
      "Effect" : "Allow"
    } ],
    "Depends" : [ {
      "catalog" : "BASE",
      "display_name" : "Server Administrator"
    }, {
      "catalog" : "BASE",
      "display_name" : "Tenant Guest"
    } ]
  }
}, {
  "domain_id" : null,
  "flag" : "fine_grained",
  "description_cn" : "Description of the permission in Chinese",
  "catalog" : "CSE",
  "name" : "system_all_34",
  "description" : "All permissions of CSE service.",
  "links" : {
    "next" : null,
    "previous" : null,
    "self" : "https://iam.myhuaweicloud.eu/v3/roles/0b5ea44ebdc64a24a9c372b2317f7..."
  },
  "id" : "0b5ea44ebdc64a24a9c372b2317f7...",
  "display_name" : "CSE Admin",
  "type" : "XA",
  "policy" : {
    "Version" : "1.1",
    "Statement" : [ {
      "Action" : [ "cse:*:*", "ecs:*:*", "evs:*:*", "vpc:*:*" ],
      "Effect" : "Allow"
    } ]
  }
} ],
"links" : {
  "next" : null,
  "previous" : null,
  "self" : "https://iam.myhuaweicloud.eu/v3/roles"
}
}
```


Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.

Error Codes

For details, see **Error Codes**.

5.8.11 Checking Whether a User Group Has Specified Permissions for All Projects

Function

This API is provided for the **administrator** to check whether a user group has specified permissions for all projects.

The API can be called using both the global endpoint and region-specific endpoints.

URI

HEAD /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects

Table 5-364 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-365 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token with **Security Administrator** permissions.

Response Parameters

None

Example Request

Request for checking whether a user group has specified permissions for all projects

```
HEAD https://iam.myhuaweicloud.eu/v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects
```

Example Response

None

Status Codes

Status Code	Description
204	The request is successful.
401	Authentication failed.
403	Access denied.
404	The server could not find the requested page.

Error Codes

For details, see **Error Codes**.

5.8.12 Removing Specified Permissions of a User Group in All Projects

Function

This API is provided for the **administrator** to remove the specified permissions of a user group for all projects.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects

Table 5-366 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-367 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token with **Security Administrator** permissions.

Response Parameters

None

Example Request

Request for removing specified permissions of a user group in all projects

```
DELETE https://iam.myhuaweicloud.eu/v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects
```

Example Response

Status code: 403

You do not have permission to perform this action.

- Example 1

```
{
  "error_code" : "IAM.0002",
```

```
  "error_msg" : "You are not authorized to perform the requested action."
}
```

- Example 2

```
{
  "error_code" : "IAM.0003",
  "error_msg" : "Policy doesn't allow %(actions)s to be performed."
}
```

Status code: 500

Internal Server Error

```
{
  "error_code" : "IAM.0006",
  "error_msg" : "An unexpected error prevented the server from fulfilling your request."
}
```

Status Codes

Status Code	Description
204	The request is successful.
401	Authentication failed.
403	You do not have permission to perform this action.
404	The server could not find the requested page.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.8.13 Removing Permissions of a User Group for a Global Service Project

Function

This API is provided for the **administrator** to remove the specified permissions of a user group for a global service project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}

Table 5-368 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-369 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for removing permissions of a user group for a global service project

```
DELETE https://iam.myhuaweicloud.eu/v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	Permissions are removed successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Error Codes

None

5.8.14 Removing the Permissions of a User Group for a Region-specific Project

Function

This API is provided for the **administrator** to remove the specified permissions of a user group for a region-specific project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}

Table 5-370 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
project_id	Yes	String	Project ID. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Parameter	Mandatory	Type	Description
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-371 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for removing permissions of a user group for a region-specific project

```
DELETE https://iam.myhuaweicloud.eu/v3/projects/{project_id}/groups/{group_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	Permissions are removed successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Error Codes

None

5.8.15 Granting Permissions to a User Group for All Projects

Function

This API is provided for the **administrator** to grant a user group permissions for all projects, including the global service project and all IAM projects.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects

Table 5-372 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
group_id	Yes	String	User group ID. For details about how to obtain a user group ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-373 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for granting permissions to a user group for all projects

```
PUT https://iam.myhuaweicloud.eu/v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects
```

Example Response

None

Status Codes

Status Code	Description
204	The authorization is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

5.9 Custom Policy Management

5.9.1 Listing Custom Policies

Function

This API is provided for the **administrator** to list all custom policies.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-ROLE/roles

Table 5-374 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number for pagination query, which must be used together with **per_page**. The minimum value is **1**.
per_page	No	Integer	Number of data records to be displayed on each page. The value ranges from 1 to 300. This parameter must be used together with **page**.

Request Parameters

Table 5-375 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-376 Parameters in the response body

Parameter	Type	Description
links	Object	Resource link information.
roles	Array of objects	Custom policy information.
total_number	Integer	Total number of custom policies returned.

Table 5-377 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-378 roles

Parameter	Type	Description
domain_id	String	Account ID.
references	Integer	Number of references.
updated_time	String	Time when the custom policy was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
created_time	String	Time when the custom policy was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description_cn	String	Description of the custom policy in Chinese.
catalog	String	Service catalog.
name	String	Name of the custom policy.
description	String	Description of the custom policy.
links	Object	Resource link of the custom policy.
id	String	Custom policy ID.
display_name	String	Display name of the custom policy.

Parameter	Type	Description
type	String	Display mode. **NOTE** • **AX**: the global service project • **XA**: region-specific projects • Set the display mode of a custom policy to either **AX** or **XA**.
policy	Object	Content of the custom policy.

Table 5-379 roles.links

Parameter	Type	Description
self	String	Resource link.

Table 5-380 roles.policy

Parameter	Type	Description
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Array of objects	Statement of the policy. A policy can contain a maximum of eight statements.

Table 5-381 roles.policy.Statement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements.
Condition	Map<String,Map<String,Array<String>>>	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**. **NOTE** Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**). `"Condition": { "StringEquals": { "obs:prefix": [ "public" ] } }`
Resource	Array of strings	Cloud resource. **NOTE** • Format: *:::::*. For example, **obs:*:bucket:***. Asterisks are allowed. • The region segment can be ***** or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Example Request

Request for querying a list of custom policies

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-ROLE/roles
```


Example Response

Status code: 200

The request is successful.


```
{
  "roles" : [ {
    "domain_id" : "d78cbac186b744899480f25bd022f...",
    "updated_time" : "1579229246886",
    "created_time" : "1579229246886",
    "description_cn" : "Description in Chinese",
    "catalog" : "CUSTOMED",
    "name" : "custom_d78cbac186b744899480f25bd022f468_1",
    "description" : "IAMDescription",
    "links" : {
      "self" : "https://iam.myhuaweicloud.eu/v3/roles/93879fd90f1046f69e6e0b31c94d2..."
    },
    "id" : "93879fd90f1046f69e6e0b31c94d2...",
    "display_name" : "IAMCloudServicePolicy",
    "type" : "AX",
    "policy" : {
      "Version" : "1.1",
      "Statement" : [ {
        "Condition" : {
          "StringStartWith" : {
            "g:ProjectName" : [ "eu-west-101" ]
          }
        },
        "Action" : [ "obs:bucket:GetBucketAcl" ],
        "Resource" : [ "obs:*:*:bucket:*" ],
        "Effect" : "Allow"
      } ]
    }
  }, {
    "domain_id" : "d78cbac186b744899480f25bd022f...",
    "updated_time" : "1579229242358",
    "created_time" : "1579229242358",
    "description_cn" : "Description in Chinese",
    "catalog" : "CUSTOMED",
    "name" : "custom_d78cbac186b744899480f25bd022f468_0",
    "description" : "IAMDescription",
    "links" : {
      "self" : "https://iam.myhuaweicloud.eu/v3/roles/f67224e84dc849ab954ce29fb4f47..."
    },
    "id" : "f67224e84dc849ab954ce29fb4f473...",
    "display_name" : "IAMAgencyPolicy",
    "type" : "AX",
    "policy" : {
      "Version" : "1.1",
      "Statement" : [ {
        "Action" : [ "iam:agencies:assume" ],
        "Resource" : {
          "uri" : [ "/iam/agencies/07805acaba800fdd4fbdc00b8f888..." ]
        },
        "Effect" : "Allow"
      } ]
    }
  } ],
  "links" : {
    "next" : null,
    "previous" : null,
    "self" : "https://iam.myhuaweicloud.eu/v3/roles?domain_id=d78cbac186b744899480f25bd022f..."
  },
  "total_number" : 300
}
```


Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
500	Internal server error.

Error Codes

None

5.9.2 Querying Custom Policy Details

Function

This API is provided for the **administrator** to query the details of a specified custom policy.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-ROLE/roles/{role_id}

Table 5-382 URI parameters

Parameter	Mandatory	Type	Description
role_id	Yes	String	Custom policy ID. For details about how to obtain a custom policy ID, see **Custom Policy ID**.

Request Parameters

Table 5-383 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-384 Parameters in the response body

Parameter	Type	Description
role	Object	Custom policy information.

Table 5-385 role

Parameter	Type	Description
domain_id	String	Account ID.
references	Integer	Number of references.
updated_time	String	Time when the custom policy was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
created_time	String	Time when the custom policy was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description_cn	String	Description of the custom policy in Chinese.
catalog	String	Service catalog.
name	String	Name of the custom policy.
description	String	Description of the custom policy.

Parameter	Type	Description
links	Object	Resource link of the custom policy.
id	String	Custom policy ID.
display_name	String	Display name of the custom policy.
type	String	Display mode. **NOTE** • **AX**: the global service project • **XA**: region-specific projects • Set the display mode of a custom policy to either **AX** or **XA**.
policy	Object	Content of the custom policy.

Table 5-386 role.links

Parameter	Type	Description
self	String	Resource link.

Table 5-387 role.policy

Parameter	Type	Description
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Array of objects	Statement of the policy. A policy can contain a maximum of eight statements.

Table 5-388 role.policy.Statement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny
Condition	Map<String,Map<String,Array<String>>>	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**. **NOTE** Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**). `"Condition": { "StringEquals": { "obs:prefix": [ "public" ] } }`
Resource	Array of strings	Cloud resource. **NOTE** • Format: *:::::*. For example, **obs:*:bucket:***. Asterisks are allowed. • The region segment can be * or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Example Request

Request for querying custom policy details

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-ROLE/roles/{role_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "role": {
        "domain_id": "d78cbac186b744899480f25bd02...",
        "references": 0,
        "description_cn": "Description in Chinese",
        "catalog": "CUSTOMED",
        "name": "custom_d78cbac186b744899480f25bd022f468_11",
        "description": "IAMDescription",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/roles/a24a71dcc41f4da989c2a1c900b52d1a"
        },
        "id": "a24a71dcc41f4da989c2a1c900b52d1a",
        "display_name": "IAMCloudServicePolicy",
        "type": "AX",
        "policy": {
            "Version": "1.1",
            "Statement": [
                {
                    "Condition": {
                        "StringStartWith": {
                            "g:ProjectName": [
                                "eu-west-101"
                            ]
                        }
                    },
                    "Action": [
                        "obs:bucket:GetBucketAcl"
                    ],
                    "Resource": [
                        "obs:*:*:bucket:*"
                    ],
                    "Effect": "Allow"
                }
            ]
        }
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.

Status Code	Description
403	Access denied.
500	Internal server error.

Error Codes

None

5.9.3 Creating a Custom Policy for Cloud Services

Function

This API is provided for the **administrator** to create a custom policy for cloud services.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3.0/OS-ROLE/roles

Request Parameters

Table 5-389 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-390 Parameters in the request body

Parameter	Mandatory	Type	Description
role	Yes	Object	Custom policy information.

Table 5-391 role

Parameter	Mandatory	Type	Description
display_name	Yes	String	Display name of the custom policy.
type	Yes	String	Application scope of the custom policy. • Global services: AX • Region-specific projects: XA Set the display mode of a custom policy to either **AX** or **XA**. **NOTE** • To assign a custom policy that contains OBS operations to a user group, create two custom policies with the scope being set to global services and region-specific projects respectively and other parameters being the same, and then attach the two policies to the user group. • To minimize the authorization scope, do not include actions of other cloud services in custom OBS policies.
description	Yes	String	Description of the custom policy.
description_cn	No	String	Description of the custom policy in Chinese.
policy	Yes	Object	Content of the custom policy.

Table 5-392 role.policy

Parameter	Mandatory	Type	Description
Version	Yes	String	Policy version. When creating a custom policy, set this parameter to **1.1**. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Yes	Array of objects	Statement of the policy. A policy can contain a maximum of eight statements.

Table 5-393 role.policy.Statement

Parameter	Mandatory	Type	Description
Action	Yes	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • A custom policy (role.policy.Statement) cannot contain actions of both project-level and global services. For details about the scope of service permissions, see **System Permissions**.
Effect	Yes	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Condition	No	Map<String,Map<String,Array<String>>>	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**.
			NOTE
			Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**).
			`"Condition": {`
			`"StringEquals": {`
			`"obs:prefix": [`
			`"public"`
			`]`
			`}`
			`}`

Parameter	Mandatory	Type	Description
Resource	No	Array of strings	Cloud resource. **NOTE** • Format: .:::: For example, **obs:.:bucket:***. Asterisks are allowed. • The region segment can be * or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists.

Response Parameters

Table 5-394 Parameters in the response body

Parameter	Type	Description
role	Object	Custom policy information.

Table 5-395 role

Parameter	Type	Description
catalog	String	Service catalog.
display_name	String	Display name of the custom policy.
description	String	Description of the custom policy.
links	Object	Resource link of the custom policy.
policy	Object	Content of the custom policy.
description_cn	String	Description of the custom policy in Chinese.
domain_id	String	Account ID.
type	String	Display mode. **NOTE** • **AX**: the global service project • **XA**: region-specific projects • Set the display mode of a custom policy to either **AX** or **XA**.
id	String	Custom policy ID.
name	String	Name of the custom policy.

Parameter	Type	Description
updated_time	String	Time when the custom policy was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
created_time	String	Time when the custom policy was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
references	String	Number of references.

Table 5-396 role.links

Parameter	Type	Description
self	String	Resource link.

Table 5-397 role.policy

Parameter	Type	Description
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Array of objects	Statement of the policy. A policy can contain a maximum of eight statements.

Table 5-398 role.policy.Statement

Parameter	Mandatory	Type	Description
Action	Yes	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations.
Effect	Yes	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Condition	No	Map<String,Map<String,Array<String>>>	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**.
			NOTE
			Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**).
			`"Condition": {`
			`"StringEquals": {`
			`"obs:prefix": [`
			`"public"`
			`]`
			`}`
			`}`

Resource	No	Array of strings	Cloud resource. **NOTE** • Format: *:::::*. For example, **obs:*:bucket:***. Asterisks are allowed. • The region segment can be ***** or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists.

Example Request

Request to create a custom policy named **IAMCloudServicePolicy** that allows only projects whose names start with **eu-west-101** to obtain ACL information about all buckets.

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-ROLE/roles
{
    "role": {
        "display_name": "IAMCloudServicePolicy",
        "type": "AX",
        "description": "IAMDescription",
        "description_cn": "Description in Chinese",
        "policy": {
            "Version": "1.1",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": [
                        "obs:bucket:GetBucketAcl"
                    ],
                    "Condition": {
                        "StringStartWith": {
                            "g:ProjectName": [
                                "eu-west-101"
                            ]
                        }
                    },
                    "Resource": [
                        "obs:*:*:bucket:*"
                    ]
                }
            ]
        }
    }
}
```

Example Response

Status code: 201

The custom policy is created successfully.

```
{
    "role": {
        "catalog": "CUSTOMED",
        "display_name": "IAMCloudServicePolicy",
        "description": "IAMDescription",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/roles/93879fd90f1046f69e6e0b31c94d2615"
        },
        "policy": {
            "Version": "1.1",
            "Statement": [
                {
                    "Action": [
                        "obs:bucket:GetBucketAcl"
                    ],
                    "Resource": [
                        "obs:*:*:bucket:*"
                    ],
                    "Effect": "Allow",
                    "Condition": {
                        "StringStartWith": {
```



```
                    "g:ProjectName": [
                        "eu-west-101"
                    ]
                }
            }
        }
    ]
  },
  "description_cn": "Description in Chinese",
  "domain_id": "d78cbac186b744899480f25bd...",
  "type": "AX",
  "id": "93879fd90f1046f69e6e0b31c9...",
  "name": "custom_d78cbac186b744899480f25bd022f468_1"
 }
}
```

Status Codes

Status Code	Description
201	The custom policy is created successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
500	Internal server error.

Error Codes

None

5.9.4 Creating a Custom Policy for Agencies

Function

This API is provided for the **administrator** to create a custom policy for agencies.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3.0/OS-ROLE/roles

Request Parameters

Table 5-399 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-400 Parameters in the request body

Parameter	Mandatory	Type	Description
role	Yes	Object	Custom policy information.

Table 5-401 role

Parameter	Mandatory	Type	Description
display_name	Yes	String	Display name of the custom policy. The value contains 1 to 64 characters.
type	Yes	String	Display mode. **NOTE** • **AX**: the global service project • **XA**: region-specific projects • Set the display mode of a custom policy to either **AX** or **XA**.
description	Yes	String	Description of the custom policy.
description_cn	No	String	Description of the custom policy in Chinese.
policy	Yes	Object	Content of the custom policy.

Table 5-402 role.policy

Parameter	Mandatory	Type	Description
Version	Yes	String	Policy version. When creating a custom policy, set this parameter to **1.1**. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Yes	Array of objects	Statement of the policy. A policy can contain a maximum of eight statements.

Table 5-403 role.policy.Statement

Parameter	Mandatory	Type	Description
Action	Yes	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*. Set this parameter to **iam:agencies:assume**.
Effect	Yes	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Parameter	Mandatory	Type	Description
Resource	Yes	Object	Resources to be managed. After an account establishes multiple trust relationships between itself and your account, you can authorize IAM users in different user groups to manage resources of the delegating party. Each IAM user can only switch to the agencies they have been authorized to access. For example: "Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}

Table 5-404 role.policy.Statement.Resource

Parameter	Mandatory	Type	Description
uri	Yes	Array of strings	URI of a delegated resource, which can contain a maximum of 128 characters. Format: /iam/agencies/*delegation ID*. For example: "uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]

Response Parameters

Table 5-405 Parameters in the response body

Parameter	Type	Description
role	Object	Custom policy information.

Table 5-406 role

Parameter	Type	Description
catalog	String	Service catalog.
display_name	String	Display name of the custom policy.
description	String	Description of the custom policy.
links	Object	Resource link of the custom policy.

Parameter	Type	Description
policy	Object	Content of the custom policy.
description_cn	String	Description of the custom policy in Chinese.
domain_id	String	Account ID.
type	String	Display mode. **NOTE** • **AX**: the global service project • **XA**: region-specific projects • Set the display mode of a custom policy to either **AX** or **XA**.
id	String	Custom policy ID.
name	String	Name of the custom policy.
updated_time	String	Time when the custom policy was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
created_time	String	Time when the custom policy was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
references	String	Number of references.

Table 5-407 role.links

Parameter	Type	Description
self	String	Resource link.

Table 5-408 role.policy

Parameter	Type	Description
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Array of objects	Statement of the policy.

Table 5-409 role.policy.Statement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny
Resource	Object	Resources to be managed. After an account establishes multiple trust relationships between itself and your account, you can authorize IAM users in different user groups to manage resources of the delegating party. Each IAM user can only switch to the agencies they have been authorized to access. For example: `"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}`

Table 5-410 role.policy.Statement.Resource

Parameter	Type	Description
uri	Array of strings	URI of a delegated resource, which can contain a maximum of 128 characters. Format: /iam/agencies/*delegation ID*. For example: `"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]`

Example Request

Request to create a custom policy with **display_name** set to **IAMAgencyPolicy** and **uri** set to **/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c**. The policy applies to global services.

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-ROLE/roles
{
    "role": {
        "display_name": "IAMAgencyPolicy",
        "type": "AX",
        "description": "IAMDescription",
        "description_cn": "Description in Chinese",
        "policy": {
            "Version": "1.1",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": [
                        "iam:agencies:assume"
                    ],
                    "Resource": {
                        "uri": [
                            "/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"
                        ]
                    }
                }
            ]
        }
    }
}
```

Example Response

Status code: 201

The custom policy for agencies is created successfully.

```
{
    "role": {
        "catalog": "CUSTOMED",
        "display_name": "IAMAgencyPolicy",
        "description": "IAMDescription",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/roles/f67224e84dc849ab954ce29fb4f47f8e"
        },
        "policy": {
            "Version": "1.1",
            "Statement": [
                {
                    "Action": [
                        "iam:agencies:assume"
                    ],
                    "Resource": {
```



```
                "uri": [
                    "/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"
                ]
            },
            "Effect": "Allow"
        }
    ]
  },
  "description_cn": "Description in Chinese",
  "domain_id": "d78cbac186b744899480f25bd02...",
  "type": "AX",
  "id": "f67224e84dc849ab954ce29fb4f47f8e",
  "name": "custom_d78cbac186b744899480f25bd022f468_0"
 }
}
```

Status Codes

Status Code	Description
201	The custom policy for agencies is created successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
500	Internal server error.

Error Codes

None

5.9.5 Modifying a Custom Policy for Cloud Services

Function

This API is provided for the **administrator** to modify a custom policy for cloud services.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PATCH /v3.0/OS-ROLE/roles/{role_id}

Table 5-411 URI parameters

Parameter	Mandatory	Type	Description
role_id	Yes	String	Custom policy ID. For details about how to obtain a custom policy ID, see **Custom Policy ID**.

Request Parameters

Table 5-412 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-413 Parameters in the request body

Parameter	Mandatory	Type	Description
role	Yes	Object	Custom policy information.

Table 5-414 role

Parameter	Mandatory	Type	Description
display_name	Yes	String	Display name of the custom policy.
type	Yes	String	Display mode. **NOTE** • **AX**: the global service project • **XA**: region-specific projects • Set the display mode of a custom policy to either **AX** or **XA**.
description	Yes	String	Description of the custom policy.

Parameter	Mandatory	Type	Description
description_cn	No	String	Description of the custom policy in Chinese.
policy	Yes	Object	Content of the custom policy.

Table 5-415 role.policy

Parameter	Mandatory	Type	Description
Version	Yes	String	Policy version. When creating a custom policy, set this parameter to **1.1**. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Yes	Array of objects	Statement of the policy. A policy can contain a maximum of eight statements.

Table 5-416 role.policy.Statement

Parameter	Mandatory	Type	Description
Action	Yes	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations.
Effect	Yes	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Condition	No	Map<String,Map<String,Array<String>>>	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**.
			NOTE
			Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**).
			`"Condition": {`
			`"StringEquals": {`
			`"obs:prefix": [`
			`"public"`
			`]`
			`}`
			`}`

Resource	No	Array of strings	Cloud resource. **NOTE** • Format: *::::*. For example, **obs:*:bucket:***. Asterisks are allowed. • The region segment can be ***** or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists.

Response Parameters

Table 5-417 Parameters in the response body

Parameter	Type	Description
role	Object	Custom policy information.

Table 5-418 role

Parameter	Type	Description
catalog	String	Service catalog.
display_name	String	Display name of the custom policy.
description	String	Description of the custom policy.
links	Object	Resource link of the custom policy.
policy	Object	Content of the custom policy.
description_cn	String	Description of the custom policy in Chinese.
domain_id	String	Account ID.
type	String	Display mode. **NOTE** • **AX**: the global service project • **XA**: region-specific projects • Set the display mode of a custom policy to either **AX** or **XA**.
id	String	Custom policy ID.
name	String	Name of the custom policy.
updated_time	String	Time when the custom policy was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.
created_time	String	Time when the custom policy was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.

Parameter	Type	Description
references	String	Number of references.

Table 5-419 role.links

Parameter	Type	Description
self	String	Resource link.

Table 5-420 role.policy

Parameter	Type	Description
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Array of objects	Statement of the policy. A policy can contain a maximum of eight statements.

Table 5-421 role.policy.Statement

Parameter	Mandatory	Type	Description
Action	Yes	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations.

Parameter	Mandatory	Type	Description
Effect	Yes	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny
Condition	No	Map<String,Map<String,Array<String>>>	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**. **NOTE** Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**). `"Condition": { "StringEquals": { "obs:prefix": [ "public" ] } }`
Resource	No	Array of strings	Cloud resource. **NOTE** • Format: *.:::*. For example, **obs:*:bucket:***. Asterisks are allowed. • The region segment can be * or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists.

Example Request

Request to modify the custom policy **IAMCloudServicePolicy** to allow only projects whose names start with **eu-west-101** to obtain ACL information about all buckets.

```
PATCH https://iam.myhuaweicloud.eu/v3.0/OS-ROLE/roles/{role_id}
{
    "role": {
        "display_name": "IAMCloudServicePolicy",
        "type": "AX",
        "description": "IAMDescription",
        "description_cn": "Description in Chinese",
        "policy": {
            "Version": "1.1",
            "Statement": [
                {
```

```
            "Effect": "Allow",
            "Action": [
               "obs:bucket:GetBucketAcl"
            ],
            "Condition": {
               "StringStartWith": {
                  "g:ProjectName": [
                     "eu-west-101"
                  ]
               }
            },
            "Resource": [
               "obs:*:*:bucket:*"
            ]
         }
      ]
   }
  }
}
```

Example Response

Status code: 200

The request is successful.

```
{
   "role": {
      "catalog": "CUSTOMED",
      "display_name": "IAMCloudServicePolicy",
      "description": "IAMDescription",
      "links": {
         "self": "https://iam.myhuaweicloud.eu/v3/roles/93879fd90f1046f69e6e0b31c94d2615"
      },
      "policy": {
         "Version": "1.1",
         "Statement": [
            {
               "Action": [
                  "obs:bucket:GetBucketAcl"
               ],
               "Resource": [
                  "obs:*:*:bucket:*"
               ],
               "Effect": "Allow",
               "Condition": {
                  "StringStartWith": {
                     "g:ProjectName": [
                        "eu-west-101"
                     ]
                  }
               }
            }
         ]
      },
      "description_cn": "Description in Chinese",
      "domain_id": "d78cbac186b744899480f25bd0...",
      "type": "AX",
      "id": "93879fd90f1046f69e6e0b31c94d2615",
      "name": "custom_d78cbac186b744899480f25bd022f468_1"
   }
}
```


Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
500	Internal server error.

Error Codes

None

5.9.6 Modifying a Custom Policy for Agencies

Function

This API is provided for the **administrator** to modify a custom policy for agencies.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PATCH /v3.0/OS-ROLE/roles/{role_id}

Table 5-422 URI parameters

Parameter	Mandatory	Type	Description
role_id	Yes	String	Custom policy ID. For details about how to obtain a custom policy ID, see **Custom Policy ID**.

Request Parameters

Table 5-423 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-424 Parameters in the request body

Parameter	Mandatory	Type	Description
role	Yes	Object	Custom policy information.

Table 5-425 role

Parameter	Mandatory	Type	Description
display_name	Yes	String	Display name of the custom policy.
type	Yes	String	Display mode. **NOTE** • **AX**: the global service project • **XA**: region-specific projects • Set the display mode of a custom policy to either **AX** or **XA**.
description	Yes	String	Description of the custom policy.
description_cn	No	String	Description of the custom policy in Chinese.
policy	Yes	Object	Content of the custom policy.

Table 5-426 role.policy

Parameter	Mandatory	Type	Description
Version	Yes	String	Policy version. When creating a custom policy, set this parameter to **1.1**. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Yes	Array of objects	Statement of the policy. A policy can contain a maximum of eight statements.

Table 5-427 role.policy.Statement

Parameter	Mandatory	Type	Description
Action	Yes	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*. Set this parameter to **iam:agencies:assume**.
Effect	Yes	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Parameter	Mandatory	Type	Description
Resource	Yes	Object	Resources to be managed. After an account establishes multiple trust relationships between itself and your account, you can authorize IAM users in different user groups to manage resources of the delegating party. Each IAM user can only switch to the agencies they have been authorized to access. For example: "Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}

Table 5-428 role.policy.Statement.Resource

Parameter	Mandatory	Type	Description
uri	Yes	Array of strings	URI of a delegated resource, which can contain a maximum of 128 characters. Format: /iam/agencies/*delegation ID*. For example: "uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]

Response Parameters

Table 5-429 Parameters in the response body

Parameter	Type	Description
role	Object	Custom policy information.

Table 5-430 role

Parameter	Type	Description
catalog	String	Service catalog.
display_name	String	Display name of the custom policy.
description	String	Description of the custom policy.
links	Object	Resource link of the custom policy.

Parameter	Type	Description
policy	Object	Content of the custom policy.
description_cn	String	Description of the custom policy in Chinese.
domain_id	String	Account ID.
type	String	Display mode. **NOTE** • **AX**: the global service project • **XA**: region-specific projects • Set the display mode of a custom policy to either **AX** or **XA**.
id	String	Custom policy ID.
name	String	Name of the custom policy.
updated_time	String	Time when the custom policy was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
created_time	String	Time when the custom policy was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
references	String	Number of references.

Table 5-431 role.links

Parameter	Type	Description
self	String	Resource link.

Table 5-432 role.policy

Parameter	Type	Description
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.
Statement	Array of objects	Statement of the policy. A policy can contain a maximum of eight statements.

Table 5-433 role.policy.Statement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny
Resource	Object	Resources to be managed. After an account establishes multiple trust relationships between itself and your account, you can authorize IAM users in different user groups to manage resources of the delegating party. Each IAM user can only switch to the agencies they have been authorized to access. For example: `"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}`

Table 5-434 role.policy.Statement.Resource

Parameter	Type	Description
uri	Array of strings	URI of a delegated resource, which can contain a maximum of 128 characters. Format: /iam/agencies/*delegation ID*. For example: `"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]`

Example Request

Request to modify the custom policy **IAMAgencyPolicy** for the agency whose URI is **/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c** to take effect for global services.

```
PATCH https://iam.myhuaweicloud.eu/v3.0/OS-ROLE/roles/{role_id}
{
   "role": {
      "display_name": "IAMAgencyPolicy",
      "type": "AX",
      "description": "IAMDescription",
      "description_cn": "Description in Chinese",
      "policy": {
         "Version": "1.1",
         "Statement": [
            {
               "Effect": "Allow",
               "Action": [
                  "iam:agencies:assume"
               ],
               "Resource": {
                  "uri": [
                     "/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"
                  ]
               }
            }
         ]
      }
   }
}
```

Example Response

Status code: 200

The request is successful.

```
{
   "role": {
      "catalog": "CUSTOMED",
      "display_name": "IAMAgencyPolicy",
      "description": "IAMDescription",
      "links": {
         "self": "https://iam.myhuaweicloud.eu/v3/roles/f67224e84dc849ab954ce29fb4f47f8e"
      },
      "policy": {
         "Version": "1.1",
         "Statement": [
            {
               "Action": [
                  "iam:agencies:assume"
               ],
               "Resource": {
```



```
                "uri": [
                    "/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"
                ]
            },
            "Effect": "Allow"
        }
    ]
  },
  "description_cn": "Description in Chinese",
  "domain_id": "d78cbac186b744899480f25b...",
  "type": "AX",
  "id": "f67224e84dc849ab954ce29fb4f47f8e",
  "name": "custom_d78cbac186b744899480f25bd022f468_0"
 }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
500	Internal server error.

Error Codes

None

5.9.7 Deleting a Custom Policy

Function

This API is provided for the **administrator** to delete a custom policy.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3.0/OS-ROLE/roles/{role_id}

Table 5-435 URI parameters

Parameter	Mandatory	Type	Description
role_id	Yes	String	Custom policy ID. For details about how to obtain a custom policy ID, see **Custom Policy ID**.

Request Parameters

Table 5-436 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for deleting a custom policy

```
DELETE https://iam.myhuaweicloud.eu/v3.0/OS-ROLE/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
200	The custom policy is deleted successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.

Status Code	Description
500	Internal server error.

Error Codes

None

5.10 Agency Management

5.10.1 Listing Agencies

Function

This API is provided for the **administrator** to list agencies that match specified conditions.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-AGENCY/agencies

Table 5-437 Query parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID of the delegating party. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. **NOTE** **domain_id** is not required if **X-Auth-Token** is set to a token with fine-grained permissions.
name	No	String	Agency name. For details about how to obtain the agency name, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Parameter	Mandatory	Type	Description
trust_domain_id	No	String	Account ID of the delegated party. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-438 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Token with **Security Administrator** permissions or policy permissions.

Response Parameters

Table 5-439 Parameters in the response body

Parameter	Type	Description
agencies	Array of objects	Agency information.

Table 5-440 agencies

Parameter	Type	Description
create_time	String	Time when the agency was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description	String	Description of the agency.
domain_id	String	ID of the delegating account.

Parameter	Type	Description
duration	String	Validity period of the agency. **FOREVER** and **null** indicate that the agency has unlimited validity. **ONEDAY** indicates that the agency is valid only for one day.
expire_time	String	Expiration time of the agency. The value **null** indicates that the agency has unlimited validity. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
id	String	Agency ID.
name	String	Agency name.
trust_domain_id	String	ID of the delegated account.
trust_domain_name	String	Name of the delegated account.

Example Request

Request for querying agencies in specified conditions

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/agencies?domain_id=0ae9c6993a2e47bb8c4c7a9bb82...
```

Example Response

Status code: 200

The request is successful.

```
{
  "agencies": [
    {
      "create_time": "2020-01-04T03:37:16.000000",
      "description": "",
      "domain_id": "d78cbac186b744899480f25b...",
      "duration": "FOREVER",
      "expire_time": null,
      "id": "0760a9e2a60026664f1fc0031f9f2...",
      "name": "IAMAgency",
      "trust_domain_id": "a2cd82a33fb043dc9304bf72...",
      "trust_domain_name": "IAMDomainB"
    }
  ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.2 Querying Agency Details

Function

This API is provided for the **administrator** to query the details about an agency.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-AGENCY/agencies/{agency_id}

Table 5-441 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-442 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Token with the **iam:agencies:getAgency** permission or **Security Administrator** permissions. For details about fine-grained permissions, see **Actions**.

Response Parameters

Table 5-443 Parameters in the response body

Parameter	Type	Description
agency	object	Agency information.

Table 5-444 agency

Parameter	Type	Description
create_time	String	Time when the agency was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description	String	Description of the agency.
domain_id	String	ID of the delegating account.
duration	String	Validity period of the agency. Unit: hour. • **FOREVER/null**: The agency has unlimited validity. • **24**: The agency is valid for 24 hours. • *XXX*: The agency has limited validity of, for example, 480 hours.

Parameter	Type	Description
expire_time	String	Expiration time of the agency. The value **null** indicates that the agency has unlimited validity. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
id	String	Agency ID.
name	String	Agency name.
trust_domain_id	String	ID of the delegated account.
trust_domain_name	String	Name of the delegated account.

Example Request

Request for querying agency details

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/agencies/{agency_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "agency":{
        "create_time":"2020-01-04T03:37:16.000000",
        "description":"",
        "domain_id":"d78cbac186b744899480f25bd...8",
        "duration":"FOREVER",
        "id":"0760a9e2a60026664f1fc0031f9f205e",
        "name":"IAMAgency",
        "trust_domain_id":"a2cd82a33fb043dc9304bf72...",
        "trust_domain_name":"IAMDomainB"
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.

Status Code	Description
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.3 Creating an Agency

Function

This API is provided for the **administrator** to create an agency.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3.0/OS-AGENCY/agencies

Request Parameters

Table 5-445 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-446 Parameters in the request body

Parameter	Mandatory	Type	Description
agency	Yes	object	Agency information.

Table 5-447 agency

Parameter	Mandatory	Type	Description
name	Yes	String	Agency name, which must contain less than or equal to 64 characters.
domain_id	Yes	String	ID of the delegating account.
trust_domain_id	No	String	ID of the delegated account. Either **trust_domain_id** or **trust_domain_name** must be specified. If both of them are specified, **trust_domain_name** takes precedence.
trust_domain_name	No	String	Name of the delegated account. Either **trust_domain_id** or **trust_domain_name** must be specified. If both of them are specified, **trust_domain_name** takes precedence.
description	No	String	Description of the agency, which must contain less than or equal to 255 characters.
duration	No	String	Validity period of the agency. Unit: day. Default value: **FOREVER**. Options: • **FOREVER**: The agency has unlimited validity. • **ONEDAY**: The agency is valid for one day. • Specific days: The agency has limited validity of, for example, 20 days.

Response Parameters

Table 5-448 Parameters in the response body

Parameter	Type	Description
agency	object	Agency information.

Table 5-449 agency

Parameter	Type	Description
create_time	String	Time when the agency was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description	String	Description of the agency.
domain_id	String	ID of the delegating account.
duration	String	Validity period of the agency. Unit: hour. • **FOREVER/null**: The agency has unlimited validity. • **24**: The agency is valid for 24 hours. • *XXX*: The agency has limited validity of, for example, 480 hours.
expire_time	String	Expiration time of the agency. **null** indicates that the agency has unlimited validity. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
id	String	Agency ID.
name	String	Agency name.
trust_domain_id	String	ID of the delegated account.
trust_domain_name	String	Name of the delegated account.

Example Request

Request to create an agency named **IAMAgency** with an unlimited validity period for the delegated account whose ID is **c2cd82a33fb043dc9304bf72a...** and whose name is **IAMDomainB**

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/agencies
{
    "agency": {
        "name": "IAMAgency",
        "domain_id": "d78cbac186b744899480f25bd...",
        "trust_domain_id": "c2cd82a33fb043dc9304bf72a...",
        "trust_domain_name": "IAMDomainB",
        "duration": "FOREVER",
        "description": "IAMDescription"
    }
}
```

Example Response

Status code: 201

The agency is created successfully.

```
{
   "agency": {
      "description": "IAMDescription",
      "trust_domain_id": "a2cd82a33fb043dc9304bf72a0f...",
      "id": "078ade0fc20010004f8fc0034fad529d",
      "duration": "FOREVER",
      "create_time": "2020-01-20T12:59:20.811642",
      "expire_time": null,
      "domain_id": "d78cbac186b744899480f25bd02...",
      "name": "IAMAgency"
   }
}
```

Status Codes

Status Code	Description
201	The agency is created successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
409	A resource conflict occurs.
500	Internal server error.

Error Codes

None

5.10.4 Modifying an Agency

Function

This API is provided for the **administrator** to modify an agency.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-AGENCY/agencies/{agency_id}

Table 5-450 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-451 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-452 Parameters in the request body

Parameter	Mandatory	Type	Description
agency	Yes	object	Agency information.

Table 5-453 agency

Parameter	Mandatory	Type	Description
trust_domain_id	No	String	ID of the delegated account. If both **trust_domain_id** and **trust_domain_name** are specified, **trust_domain_name** takes precedence. At least one of these four parameters must be specified for the agency.

Parameter	Mandatory	Type	Description
trust_domain_name	No	String	Name of the delegated account. If both **trust_domain_id** and **trust_domain_name** are specified, **trust_domain_name** takes precedence. At least one of these four parameters must be specified for the agency.
description	No	String	Description of the agency, which must contain less than or equal to 255 characters. At least one of these four parameters must be specified for the agency.
duration	No	String	Validity period of the agency. Unit: day. At least one of these four parameters must be specified for the agency. Options: • **FOREVER**: The agency has unlimited validity. • **ONEDAY**: The agency is valid for one day. • Specific days: The agency is valid for a specific number of days, for example, 20 days.

Response Parameters

Table 5-454 Parameters in the response body

Parameter	Type	Description
agency	object	Agency information.

Table 5-455 agency

Parameter	Type	Description
create_time	String	Time when the agency was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
description	String	Description of the agency.
domain_id	String	ID of the delegating account.
duration	String	Validity period of the agency. Unit: hour. • **FOREVER/null**: The agency has unlimited validity. • **24**: The agency is valid for 24 hours. • *XXX*: The agency has limited validity of, for example, 480 hours.
expire_time	String	Expiration time of the agency. The value **null** indicates that the agency has unlimited validity. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
id	String	Agency ID.
name	String	Agency name.
trust_domain_id	String	ID of the delegated account.
trust_domain_name	String	Name of the delegated account.

Example Request

Request for changing the validity period of an agency to one day.

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/agencies/{agency_id}
{
    "agency": {
        "trust_domain_id": "b2cd82a33fb043dc9304bf72...",
        "trust_domain_name": "IAMDomainB",
        "description": "IAMDescription",
        "duration": "ONEDAY"
    }
}
```

Example Response

Status code: 200

The agency is modified successfully.

```
{
    "agency": {
        "description": "IAMDescription",
        "trust_domain_id": "b2cd82a33fb043dc9304bf72a0...",
        "id": "0760a9e2a60026664f1fc0031f9f205e",
        "duration": "ONEDAY",
        "create_time": "2020-01-04T03:37:16.000000",
        "expire_time": "2020-01-21T13:06:11.241588",
        "domain_id": "d78cbac186b744899480f25...",
        "name": "IAMAgency"
    }
}
```

Status Codes

Status Code	Description
200	The agency is modified successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.5 Deleting an Agency

Function

This API is provided for the **administrator** to delete an agency.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3.0/OS-AGENCY/agencies/{agency_id}

Table 5-456 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-457 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for deleting an agency

```
DELETE https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/agencies/{agency_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The agency is deleted successfully.
401	Authentication failed.
403	Access denied.

Status Code	Description
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.6 Querying Permissions of an Agency for a Global Service Project

Function

This API is provided for the **administrator** to query the permissions of an agency for a global service project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles

Table 5-458 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_id	Yes	String	Account ID of the delegating party. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-459 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-460 Parameters in the response body

Parameter	Type	Description
roles	Array of objects	Permission information.

Table 5-461 roles

Parameter	Type	Description
domain_id	String	ID of the account to which the permission belongs.
flag	String	If this parameter is set to **fine_grained**, the permission is a system-defined policy.
description_cn	String	Description of the permission in Chinese.
catalog	String	Service catalog of the permission.
name	String	Permission name. This parameter is carried in the token of a user, allowing the system to determine whether the user has permissions to access a specific cloud service.
description	String	Description of the permission.
links	Object	Permission resource link.
id	String	Permission ID.
display_name	String	Display name of the permission.

Parameter	Type	Description
type	String	Display mode of the permission. **NOTE** • **AX**: Account level. • **XA**: Project level. • **AA**: Both the account level and project level. • **XX**: Neither the account level nor project level. • The display mode of a custom policy can only be **AX** or **XA**. A custom policy must be displayed at either of the two levels.
policy	Object	Content of the permission.
updated_time	String	Time when the permission was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
created_time	String	Time when the permission was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Table 5-462 roles.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-463 roles.policy

Parameter	Type	Description
Depends	Array of objects	Dependent permissions.
Statement	Array of objects	Statement of the permission.

Parameter	Type	Description
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.

Table 5-464 roles.policy.Depends

Parameter	Type	Description
catalog	String	Service catalog of the permission.
display_name	String	Display name of the permission.

Table 5-465 roles.policy.Statement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny

Parameter	Type	Description
Condition	Object	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**. **NOTE** Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**). `"Condition": { "StringEquals": { "obs:prefix": [ "public" ] } }`
Resource	Array of strings	Cloud resource. **NOTE** • Format: *:::::*. For example, **obs:::bucket:***. Asterisks are allowed. • The region segment can be ***** or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Example Request

Request for querying permissions of an agency for a global service project

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles
```

Example Response

Status code: 200

The request is successful.


```
{
    "roles": [
        {
            "flag": "fine_grained",
            "display_name": "CDN Domain Viewer",
            "description": "Allow Query Domains",
            "name": "system_all_11",
            "policy": {
                "Version": "1.1",
                "Statement": [
                    {
                        "Action": [
                            "cdn:configuration:queryDomains",
                            "cdn:configuration:queryOriginServerInfo",
                            "cdn:configuration:queryOriginConfInfo",
                            "cdn:configuration:queryHttpsConf",
                            "cdn:configuration:queryCacheRule",
                            "cdn:configuration:queryReferConf",
                            "cdn:configuration:queryChargeMode",
```



```
                    "cdn:configuration:queryCacheHistoryTask",
                    "cdn:configuration:queryIpAcl",
                    "cdn:configuration:queryResponseHeaderList"
                ],
                "Effect": "Allow"
            }
        ]
    },
    "description_cn": "Description of the permission in Chinese",
    "domain_id": null,
    "type": "AX",
    "catalog": "CDN",
    "id": "db4259cce0ce47c9903dfdc195eb453b"
  }
 ]
}
```


Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.7 Querying Permissions of an Agency for a Region-specific Project

Function

This API is provided for the **administrator** to query the permissions of an agency for a region-specific project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles

Table 5-466 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
project_id	Yes	String	Project ID of the delegating party. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-467 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-468 Parameters in the response body

Parameter	Type	Description
roles	Array of objects	Permission information.

Table 5-469 roles

Parameter	Type	Description
domain_id	String	ID of the account to which the permission belongs.

Parameter	Type	Description
flag	String	If this parameter is set to **fine_grained**, the permission is a system-defined policy.
description_cn	String	Description of the permission in Chinese.
catalog	String	Service catalog of the permission.
name	String	Permission name. This parameter is carried in the token of a user, allowing the system to determine whether the user has permissions to access a specific cloud service.
description	String	Description of the permission.
links	Object	Permission resource link.
id	String	Permission ID.
display_name	String	Display name of the permission.
type	String	Display mode of the permission. **NOTE** • **AX**: Account level. • **XA**: Project level. • **AA**: Both the account level and project level. • **XX**: Neither the account level nor project level. • The display mode of a custom policy can only be **AX** or **XA**. A custom policy must be displayed at either of the two levels.
policy	Object	Content of the permission.
updated_time	String	Time when the permission was last updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
created_time	String	Time when the permission was created. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Table 5-470 roles.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.

Parameter	Type	Description
next	String	Next resource link.

Table 5-471 roles.policy

Parameter	Type	Description
Depends	Array of objects	Dependent permissions.
Statement	Array of objects	Statement of the permission.
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.

Table 5-472 roles.policy.Depends

Parameter	Type	Description
catalog	String	Service catalog of the permission.
display_name	String	Display name of the permission.

Table 5-473 roles.policy.Statement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.

Parameter	Type	Description
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Options: • Allow • Deny
Condition	Object	Conditions for the permission to take effect. For details, see **Creating a Custom Policy**. **NOTE** Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**). `"Condition": { "StringEquals": { "obs:prefix": [ "public" ] } }`
Resource	Array of strings	Cloud resource. **NOTE** • Format: *:::::*. For example, **obs:::bucket:***. Asterisks are allowed. • The region segment can be * or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Example Request

Request for querying permissions of an agency for a region-specific project

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles
```

Example Response

Status code: 200

The request is successful.

```
{
    "roles": [
        {
            "domain_id": null,
            "flag": "fine_grained",
            "description_cn": "Description of the permission in Chinese",
```



```
        "catalog": "AOM",
        "name": "system_all_30",
        "description": "AOM read only",
        "id": "75cfe22af2b3498d82b655fbb39de498",
        "display_name": "AOM Viewer",
        "type": "XA",
        "policy": {
            "Version": "1.1",
            "Statement": [
                {
                    "Action": [
                        "aom:*:list",
                        "aom:*:get",
                        "apm:*:list",
                        "apm:*:get"
                    ],
                    "Effect": "Allow"
                }
            ]
        }
    }
  ]
}
```


Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.8 Granting Permissions to an Agency for a Global Service Project

Function

This API is provided for the **administrator** to grant permissions to an agency for a global service project.

The API can be called using both the global endpoint and region-specific endpoints.

Restrictions

The permission with the **role_id** specified in the URL will be controlled through the blacklist. The **role_id** cannot be set to **te_agency**.

URI

PUT /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}

Table 5-474 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_id	Yes	String	Account ID of the delegating party. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Global service permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-475 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for granting permissions to an agency for a global service project

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The authorization is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.9 Granting Permissions to an Agency for a Region-specific Project

Function

This API is provided for the **administrator** to grant permissions to an agency for a region-specific project.

The API can be called using both the global endpoint and region-specific endpoints.

Restrictions

The permission with the **role_id** specified in the URL will be controlled through the blacklist and cannot be specified as **secu_admin** or **te_agency**.

URI

PUT /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}

Table 5-476 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
project_id	Yes	String	Project ID of the delegating party. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Project-level service permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-477 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for granting permissions to an agency for a region-specific project

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The authorization is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.10 Checking Whether an Agency Has Specified Permissions for a Global Service Project

Function

This API is provided for the **administrator** to check whether an agency has specified permissions for a global service project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

HEAD /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}

Table 5-478 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_id	Yes	String	Account ID of the delegating party. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Parameter	Mandatory	Type	Description
role_id	Yes	String	Global service permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-479 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for checking whether an agency has specified permissions for a global service project

```
HEAD https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The request is successful. (The agency has the specified permissions for the global service project.)
401	Authentication failed.
403	Access denied.

Status Code	Description
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.11 Checking Whether an Agency Has Specified Permissions for a Region-specific Project

Function

This API is provided for the **administrator** to check whether an agency has specified permissions for a region-specific project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}

Table 5-480 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
project_id	Yes	String	Project ID of the delegating party. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Project-level service permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-481 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Authenticated token with **Security Administrator** permissions.

Response Parameters

None

Example Request

Request for checking whether an agency has specified permissions for a region-specific project

```
HEAD https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The request is successful. (The agency has the specified permissions for the region-specific project.)
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.12 Removing Permissions of an Agency for a Global Service Project

Function

This API is provided for the **administrator** to remove the specified permissions of an agency for a global service project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}

Table 5-482 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_id	Yes	String	Account ID of the delegating party. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Global service permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-483 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for removing permissions of an agency for a global service project

```
DELETE https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	Permissions are removed successfully.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.13 Removing Permissions of an Agency for a Region-specific Project

Function

This API is provided for the **administrator** to remove the specified permissions of an agency for a region-specific project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}

Table 5-484 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
project_id	Yes	String	Project ID of the delegating party. For details about how to obtain the project ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Project-level service permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-485 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for removing permissions of an agency for a region-specific project

```
DELETE https://iam.myhuaweicloud.eu/v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	Permissions are removed successfully.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

None

5.10.14 Querying All Permissions of an Agency

Function

This API is provided for the **administrator** to query all permissions that have been assigned to an agency.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects

Table 5-486 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_id	Yes	String	Account ID of the delegating party. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-487 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-488 Parameters in the response body

Parameter	Type	Description
roles	Array of objects	Permission information.
links	object	Resource link information.

Table 5-489 roles

Parameter	Type	Description
id	String	Permission ID.
links	object	Permission resource link.
name	String	Permission name.

Table 5-490 links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for querying all permissions of an agency

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects
```

Example Response

Status code: 200

The request is successful.


```
{
  "roles" : [
    {
      "name" : "system_all_154",
      "links" : {
                  "self" : "https://internal.iam.ctcclouddev.com/v3/roles/04570dfe267c45a3940e1ae9de868..."
                },
      "id" : "04570dfe267c45a3940e1ae9de868..."
    },
    {
      "name" : "test1_admin",
      "links" : {
                   "self" : "https://internal.iam.ctcclouddev.com/v3/roles/1bf20f1adba94747a6e02e1be3810..."
                  },
      "id" : "1bf20f1adba94747a6e02e1be3810..."
    }
  ],
  "links" : {
      "self" : "https://internal.iam.ctcclouddev.com/v3.0/OSHERIT/domains/
05b09b4723001dc90f27c0008f8b1.../agencies/08c6652e86801d234f01c00078308.../roles/
inherited_to_projects"
        }
}
```


Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.10.15 Granting Specified Permissions to an Agency for All Projects

Function

This API is provided for the **administrator** to grant specified permissions to an agency for all projects.

The API can be called using both the global endpoint and region-specific endpoints.

Restrictions

The permission with the **role_id** specified in the URL is controlled through the blacklist and cannot be set to **te_agency**.

URI

PUT /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects

Table 5-491 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_id	Yes	String	Account ID of the delegating party. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-492 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for granting specified permissions to an agency for all projects

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects
```

Example Response

None

Status Codes

Status Code	Description
204	The authorization is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.10.16 Checking Whether an Agency Has Specified Permissions

Function

This API is provided for the **administrator** to check whether an agency has specified permissions.

The API can be called using both the global endpoint and region-specific endpoints.

URI

HEAD /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects

Table 5-493 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_id	Yes	String	Account ID of the delegating party. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-494 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for checking whether an agency has specified permissions

```
HEAD https://iam.myhuaweicloud.eu/v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects
```

Example Response

None

Status Codes

Status Code	Description
204	The request is successful. (The agency has the specified permissions.)
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.10.17 Removing Specified Permissions of an Agency in All Projects

Function

This API is provided for the **administrator** to remove the specified permissions of an agency in all projects.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects

Table 5-495 URI parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID. For details about how to obtain the agency ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
domain_id	Yes	String	Account ID of the delegating party. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Parameter	Mandatory	Type	Description
role_id	Yes	String	Permission ID. For details about how to obtain a permission ID, see **Listing Permissions**.

Request Parameters

Table 5-496 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for removing specified permissions of an agency in all projects

```
DELETE https://iam.myhuaweicloud.eu/v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects
```

Example Response

None

Status Codes

Status Code	Description
204	Permissions are removed successfully.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.11 Enterprise Project Management

5.11.1 Querying User Groups Associated with an Enterprise Project

Function

This API is used to query the user groups directly associated with a specified enterprise project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups

Table 5-497 URI parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	ID of the enterprise project for querying the permissions of an associated user group.

Request Parameters

Table 5-498 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:listGroupsOnEnterpriseProject** or **Security Administrator** permission. The **domain_id** of the account to which the **enterprise_project_id** belongs must be the same as the **domain_id** in the token.

Response Parameters

Status code: 200

Table 5-499 Parameters in the response body

Parameter	Type	Description
groups	Array of objects	User group information.

Table 5-500 ListGroupsForEnterpriseProjectResDetail

Parameter	Type	Description
createTime	Integer	Time when the user group was created.
description	String	User group description.
domainId	String	Account ID.
id	String	User group ID.
name	String	User group name.

Example Request

Request for querying user groups associated with an enterprise project

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups
```

Example Response

Status code: 200

The request is successful.

```
{
  "groups" : [ {
    "createTime" : 1552093271000,
    "description" : null,
    "domainId" : "dc7f62ae236c47b8836014c16d64d...",
    "id" : "e6bde2403bda43e2813a1a6848963...",
    "name" : "auth"
  } ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Parameter error.
401	Authentication failed.
403	Access denied.

Status Code	Description
404	The requested resource cannot be found.
415	Incorrect Content-Type.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.11.2 Querying the Permissions of a User Group Associated with an Enterprise Project

Function

This API is used to query the permissions of a user group directly associated with a specified enterprise project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles

Table 5-501 URI parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	ID of the enterprise project for querying the permissions of an associated user group.
group_id	Yes	String	User group ID.

Request Parameters

Table 5-502 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:listRolesForGroupOnEnterpriseProject** or **Security Administrator** permissions. The **domain_id** of the account to which the **group_id** belongs must be the same as the **domain_id** in the token.

Response Parameters

Status code: 200

Table 5-503 Parameters in the response body

Parameter	Type	Description
roles	Array of objects	Role list.

Table 5-504 roles

Parameter	Type	Description
catalog	String	Service catalog of the permission.
display_name	String	Display name of the permission.
description	String	Description of the permission in English.
description_cn	String	Description of the permission in Chinese.
domain_id	String	ID of the account to which the permission belongs.
flag	String	If this parameter is set to **fine_grained**, the permission is a system-defined policy.
id	String	Permission ID.
name	String	Permission name.
policy	object	Content of the permission.

Parameter	Type	Description
type	String	Display mode of the permission. **NOTE** • **AX**: Account level. • **XA**: Project level. • **AA**: Both the account level and project level. • **XX**: Neither the account level nor project level. • The display mode of a custom policy can only be **AX** or **XA**. A custom policy must be displayed at either of the two levels.

Table 5-505 RolePolicy

Parameter	Type	Description
Depends	Array of objects	Dependent permissions.
Statement	Array of objects	Statement of the permission.
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.

Table 5-506 PolicyDepends

Parameter	Type	Description
catalog	String	Service catalog of the permission.
display_name	String	Display name of the permission.

Table 5-507 PolicyStatement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements. Enumerated values: • Allow • Deny

Condition	Object	Conditions for the permission to take effect. For details about the condition parameters, see **Creating a Custom Policy**.
		NOTE
		Take the condition in the sample request as an example, the values of the condition key (**obs:prefix**) and string (**public**) must be equal (**StringEquals**).
		`"Condition": {`
		`"StringEquals": {`
		`"obs:prefix": [`
		`"public"`
		`]`
		`}`
		`}`

Resource	Array of strings	Cloud resource. **NOTE** • Format: *::::*. For example, **obs:*:*:bucket:***. Asterisks are allowed. • The region segment can be * or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Example Request

Request for querying the permissions of a user group associated with an enterprise project

```
GET  https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/
groups/{group_id}/roles
```

Example Response

Status code: 200

The request is successful.

```
{
  "roles" : [ {
    "catalog" : "CUSTOMED",
    "description" : "u81eau5b9au4e49u6743u9...",
    "description_cn" : null,
    "display_name" : "XpBdkPYCCx",
    "domain_id" : "0456fd5a278033120f37c006683ab...",
    "flag" : null,
    "id" : "5d1b6256331f4fb494534bf240698...",
    "name" : "custom_policy1",
    "policy" : {
      "Statement" : [ {
        "Action" : [ "aaa:a*b:baa*" ],
        "Condition" : null,
        "Effect" : "deny",
        "Resource" : null
      }, {
        "Action" : [ "aaa:a*b:bab*" ],
        "Condition" : null,
        "Effect" : "Allow",
        "Resource" : null
      } ],
      "Version" : "1.1"
    },
    "type" : "XA"
  } ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Parameter error.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
415	Incorrect Content-Type.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.11.3 Granting Permissions to a User Group Associated with an Enterprise Project

Function

This API is used to grant permissions to a user group associated with the enterprise project of a specified ID.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}

Table 5-508 URI parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	Enterprise project ID.
group_id	Yes	String	User group ID.
role_id	Yes	String	Role ID. **NOTE** Ensure that the role you specify can be used for authorization by enterprise project. For details, see **Supported Cloud Services**.

Request Parameters

Table 5-509 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:grantRoleToGroupOnEnterpriseProject** or **Security Administrator** permissions. The **domain_id** of the account to which the **group_id** belongs must be the same as the **domain_id** in the token.

Response Parameters

None

Example Request

Request for granting permissions to a user group associated with an enterprise project

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The request is successful.
400	The request message is invalid.
401	Token authentication failed.
403	Access denied.
415	Incorrect Content-Type.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.11.4 Removing Permissions of a User Group Associated with an Enterprise Project

Function

This API is used to remove the permissions of a user group associated with an enterprise project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}

Table 5-510 URI parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	Enterprise project ID.
group_id	Yes	String	User group ID.
role_id	Yes	String	Permission ID.

Request Parameters

Table 5-511 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:revokeRoleFromGroupOnEnterpriseProject** or **Security Administrator** permissions. The **domain_id** of the account to which the **group_id** belongs must be the same as the **domain_id** in the token.

Response Parameters

None

Example Request

Request for removing permissions of a user group associated with an enterprise project

```
DELETE https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The request is successful.
400	The request message is invalid.

Status Code	Description
401	Token authentication failed.
403	Access denied.
404	The resource does not exist.
415	Incorrect Content-Type.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.11.5 Querying the Enterprise Projects Associated with a User Group

Function

This API is used to query the enterprise projects associated with a user group.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-PERMISSION/groups/{group_id}/enterprise-projects

Table 5-512 URI parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	User group ID.

Request Parameters

Table 5-513 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:listEnterpriseProjectsForGroup** or **Security Administrator** permission. The **domain_id** of the account to which the **group_id** belongs must be the same as the **domain_id** in the token.

Response Parameters

Status code: 200

Table 5-514 Parameters in the response body

Parameter	Type	Description
enterprise-projects	Array of objects	Enterprise project information.

Table 5-515 ListEnterpriseProjectsResDetail

Parameter	Type	Description
projectId	String	Project ID.

Example Request

Request for querying enterprise projects associated with a user group

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/groups/{group_id}/enterprise-projects
```

Example Response

Status code: 200

The request is successful.

```
{
  "enterprise-projects" : [ {
    "projectId" : "dd87a1a8-8602-45a8-8145-393af4c95..."
  } ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Parameter error.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
415	Incorrect Content-Type.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.11.6 Querying the Enterprise Projects Directly Associated with an IAM User

Function

This API is used to query the enterprise projects directly associated with an IAM user.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-PERMISSION/users/{user_id}/enterprise-projects

Table 5-516 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Request Parameters

Table 5-517 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:listEnterpriseProjectsForUser** or **Security Administrator** permission. The **domain_id** of the account to which the **user_id** belongs must be the same as the **domain_id** in the token.

Response Parameters

Status code: 200

Table 5-518 Parameters in the response body

Parameter	Type	Description
enterprise-projects	Array of objects	Enterprise project information.

Table 5-519 enterprise-projects

Parameter	Type	Description
projectId	String	Project ID.

Example Request

Request for querying enterprise projects directly associated with an IAM user

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/users/{user_id}/enterprise-projects
```

Example Response

Status code: 200

The request is successful.

```
{
  "enterprise-projects" : [ {
    "projectId" : "dd87a1a8-8602-45a8-8145-393af4c95..."
  }, {
    "projectId" : "dd87a1a8-8602-45a8-8145-393af4c95..."
  } ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Parameter error.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
415	Incorrect Content-Type.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.11.7 Querying Users Directly Associated with an Enterprise Project

Function

This API is used to query the users directly associated with a specified enterprise project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users

Table 5-520 URI parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	ID of the enterprise project to be queried.

Request Parameters

Table 5-521 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:listUsersForEnterpriseProject** or **Security Administrator** permission.

Response Parameters

Status code: 200

Table 5-522 Parameters in the response body

Parameter	Type	Description
users	Array of objects	User information.

Table 5-523 users

Parameter	Type	Description
domain_id	String	ID of the account to which an authorized user belongs.
id	String	ID of the authorized user.
name	String	Name of the authorized user.
enabled	Boolean	Indicates whether the authorized user is enabled. The value can be **true** or **false**. The default value is **true**.
description	String	Description of the authorized user.
policy_num	Integer	Number of policies that have been assigned to the authorized user.
lastest_policy_time	Long	Duration for which the user has been last associated with a policy in the enterprise project.

Example Request

Request for querying users associated with an enterprise project

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users
```

Example Response

Status code: 200

The request is successful.

```
{
  "users" : [ {
    "domain_id" : "d78cbac186b744899480f25bd02...",
    "id" : "07667db96a00265f1fc0c003a...",
    "name" : "IAMUserA",
    "enabled" : true,
    "description" : "IAMDescriptionA",
    "policy_num" : 2,
    "lastest_policy_time" : 1589874427000
  } ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Parameter error.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	The system is abnormal.

5.11.8 Querying Permissions of a User Directly Associated with an Enterprise Project

Function

This API is used to query the permissions of a user directly associated with a specified enterprise project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles

Table 5-524 URI parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	Enterprise project ID.
user_id	Yes	String	User ID.

Request Parameters

Table 5-525 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:listRolesForUserOnEnterpriseProject** or **Security Administrator** permissions.

Response Parameters

Status code: 200

Table 5-526 Parameters in the response body

Parameter	Type	Description
roles	Array of objects	Role list.

Table 5-527 RolesItem

Parameter	Type	Description
catalog	String	Service catalog of the permission.
display_name	String	Display name of the permission.
description	String	Description of the permission in English.
description_cn	String	Description of the permission in Chinese.
domain_id	String	ID of the account to which the permission belongs.
flag	String	If this parameter is set to **fine_grained**, the permission is a system-defined policy.

Parameter	Type	Description
id	String	Permission ID.
name	String	Permission name.
policy	object	Content of the permission.
type	String	Display mode of the permission. **NOTE** • **AX**: Account level. • **XA**: Project level. • **AA**: Both the account level and project level. • **XX**: Neither the account level nor project level. • The display mode of a custom policy can only be **AX** or **XA**. A custom policy must be displayed at either of the two levels.

Table 5-528 RolePolicy

Parameter	Type	Description
Depends	Array of objects	Dependency permissions.
Statement	Array of objects	Statement of the permission.
Version	String	Policy version. **NOTE** • **1.0**: System-defined role. Only a limited number of service-level roles are provided for authorization. • **1.1**: Policy. A policy defines the permissions required to perform operations on a specific cloud resource under certain conditions.

Table 5-529 PolicyDepends

Parameter	Type	Description
catalog	String	Service catalog of the permission.
display_name	String	Display name of the permission.

Table 5-530 PolicyStatement

Parameter	Type	Description
Action	Array of strings	Specific operation permissions on a resource. For details about supported actions, see "Permissions and Supported Actions" in the API Reference of cloud services. **NOTE** • The value format is *Service name*:*Resource type*:*Operation*, for example, **vpc:ports:create**. • *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. Resource types and operations are not case-sensitive. You can use an asterisk (*) to represent all operations. • In the case of a custom policy for agencies, this parameter should be set to *"Action": ["iam:agencies:assume"]*.
Effect	String	Effect of the permission. The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements.
Condition	Object	Conditions for the permission to take effect.
Resource	Array of strings	Cloud resource. **NOTE** • Format: *::::*. For example, **obs:*:bucket:***. Asterisks are allowed. • The region segment can be ***** or a region accessible to the user. The specified resource must belong to the corresponding service that actually exists. • In the case of a custom policy for agencies, the type of this parameter is Object, and the value should be set to *"Resource": {"uri": ["/iam/agencies/07805acaba800fdd4fbdc00b8f888c7c"]}*.

Example Request

Request for querying permissions of a user directly associated with an enterprise project

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles
```

Example Response

Status code: 200

The request is successful.


```
{
  "roles" : [ {
    "display_name" : "Customed ECS Viewer",
    "description" : "The read-only permissions to all ECS resources, which can be used for statistics and
survey.",
    "domain_id" : "9698542758bc422088c0c3eabfc30d...",
    "catalog" : "CUSTOMED",
    "policy" : {
      "Version" : "1.1",
      "Statement" : [ {
        "Action" : [ "ecs:*:get*", "ecs:*:list*", "ecs:blockDevice:use", "ecs:serverGroups:manage",
"ecs:serverVolumes:use", "evs:*:get*", "evs:*:list*", "vpc:*:get*", "vpc:*:list*", "ims:*:get*", "ims:*:list*" ],
        "Effect" : "Allow"
      } ]
    },
    "id" : "24e7a89bffe443979760c4e9715c1...",
    "type" : "XA",
    "name" : "custom_9698542758bc422088c0c3eabfc30...."
  } ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Parameter error.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	The system is abnormal.

5.11.9 Granting a User Permissions for an Enterprise Project

Function

This API is used to grant a user permissions for a specified enterprise project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}

Table 5-531 URI parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	Enterprise project ID.
user_id	Yes	String	User ID.
role_id	Yes	String	Permission ID.

Request Parameters

Table 5-532 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:grantRoleToUserOnEnterpriseProject** or **Security Administrator** permissions.

Response Parameters

None

Example Request

Request for granting permissions to a user associated with an enterprise project

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}
```

Example Response

Status code: 400

Parameter error.

```
{
  "error" : {
    "message" : "Illegal request",
    "code" : 400,
    "title" : "Bad Request"
  }
}
```

Status code: 401

Authentication failed.

```
{
  "error" : {
    "message" : "Authentication failed",
    "code" : 401,
```

```
    "title" : "Unauthorized"
  }
}
```

Status code: 403

Access denied.

```
{
  "error" : {
    "message" : "Forbidden operation",
    "code" : 403,
    "title" : "Forbidden"
  }
}
```

Status Codes

Status Code	Description
204	The request is successful.
400	Parameter error.
401	Authentication failed.
403	Access denied.
500	The system is abnormal.

5.11.10 Removing Permissions of a User Directly Associated with an Enterprise Project

Function

This API is used to remove the permissions of a user directly associated with a specified enterprise project.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}

Table 5-533 URI parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	Enterprise project ID.
user_id	Yes	String	User ID.

Parameter	Mandatory	Type	Description
role_id	Yes	String	Permission ID.

Request Parameters

Table 5-534 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:revokeRoleFromUserOnEnterpriseProject** or **Security Administrator** permissions.

Response Parameters

None

Example Request

Request for deleting roles of a user associated with an enterprise project

```
DELETE https://iam.myhuaweicloud.eu/v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The request is successful.
400	Parameter error.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	The system is abnormal.

5.11.11 Granting Permissions to Agencies Associated with Specified Enterprise Projects

Function

This API is used to grant permissions to agencies associated with specified enterprise projects.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments

Request Parameters

Table 5-535 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **iam:permissions:grantRoleToAgencyOnEnterpriseProject** or **Security Administrator** permissions.

Table 5-536 Parameters in the request body

Parameter	Mandatory	Type	Description
role_assignments	Yes	Array of objects	Association between agencies and enterprise projects. A maximum of 250 association records are supported.

Table 5-537 role_assignments

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID.
enterprise_project_id	Yes	String	Enterprise project ID.

Parameter	Mandatory	Type	Description
role_id	Yes	String	Policy ID.

Response Parameters

None

Example Request

Request for granting permissions to agencies associated with a specified enterprise project

```
PUT /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments
{
  "role_assignments": [
    {
      "agency_id": "as0d9f8asdfasdfa09sd8f9aaa",
      "enterprise_project_id": "3asdfs0d9f8asdfasdfa09sd8f9aaa",
      "role_id": "5s0d9f8dafsdfasdfa09sd8f9aaa"
    }
  ]
}
```

Example Response

Status code: 200

The request is successful.

Status code: 400

Parameter error.

```
{
  "error" : {
    "message" : "Illegal request",
    "code" : 400,
    "title" : "Bad Request"
  }
}
```

Status code: 401

Authentication failed.

```
{
  "error" : {
    "message" : "Authentication failed",
    "code" : 401,
    "title" : "Unauthorized"
  }
}
```

Status code: 403

Operation denied.


```
{
  "error" : {
    "message" : "Forbidden operation",
    "code" : 403,
    "title" : "Forbidden"
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Parameter error.
401	Authentication failed.
403	Unauthorized operation.
500	Internal server error.

5.11.12 Removing Permissions of Agencies Associated with Specified Enterprise Projects

Function

This API is used to remove permissions of agencies associated with specified enterprise projects.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments

Request Parameters

Table 5-538 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with the **iam:permissions:revokeRoleFromAgencyOnEnterpriseProject** fine-grained permissions or the **Security Administrator** permissions.

Table 5-539 Parameters in the request body

Parameter	Mandatory	Type	Description
role_assignments	Yes	Array of objects	Association between agencies and enterprise projects. A maximum of 250 association records are supported.

Table 5-540 role_assignments

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency ID.
enterprise_project_id	Yes	String	Enterprise project ID.
role_id	Yes	String	Policy ID.

Response Parameters

None

Example Request

Request for removing permissions of agencies associated with a specified enterprise project

```
DELETE /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments
{
  "role_assignments": [
    {
      "agency_id": "as0d9f8asdfasdfa09sd8f9aaa",
      "enterprise_project_id": "3asdfs0d9f8asdfasdfa09sd8f9aaa",
      "role_id": "5s0d9f8dafsdfasdfa09sd8f9aaa"
    }
  ]
}
```

Example Response

Status code: 204

The request is successful.

Status code: 400

Parameter error.

```
{
  "error" : {
```

```
    "message" : "Illegal request",
    "code" : 400,
    "title" : "Bad Request"
  }
}
```

Status code: 401

Authentication failed.

```
{
  "error" : {
    "message" : "Authentication failed",
    "code" : 401,
    "title" : "Unauthorized"
  }
}
```

Status code: 403

Operation denied.

```
{
  "error" : {
    "message" : "Forbidden operation",
    "code" : 403,
    "title" : "Forbidden"
  }
}
```

Status Codes

Status Code	Description
204	The request is successful.
400	Parameter error.
401	Authentication failed.
403	Unauthorized operation.
500	Internal server error.

5.12 Security Settings

5.12.1 Modifying the Operation Protection Policy

Function

This API is provided for the **administrator** to modify the operation protection policy.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy

Table 5-541 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-542 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-543 Parameter in the request body

Parameter	Mandatory	Type	Description
protect_policy	Yes	ProtectPolicyOption object	Specifies the operation protection policy.

Table 5-544 protect_policy

Parameter	Mandatory	Type	Description
operation_protection	Yes	boolean	Specifies whether to enable operation protection. The value can be **true** or **false**.

Parameter	Mandatory	Type	Description
allow_user	No	AllowUserBody object	Specifies the attributes IAM users can modify.
mobile	No	string	Specifies the mobile number used for verification. Example:
admin_check	No	string	Specifies whether to designate a person for verification. If this parameter is set to **on**, you need to specify the **scene** parameter to designate a person for verification. If this parameter is set to **off**, the designated operator is responsible for verification.
email	No	string	Specifies the email address used for verification. An example value is example@email.com.
scene	No	string	Specifies the verification method. This parameter is mandatory when **admin_check** is set to **on**. The value options are **mobile** and **email**.

Table 5-545 protect_policy.allow_user

Parameter	Mandatory	Type	Description
manage_accesskey	No	boolean	Specifies whether to allow IAM users to manage access keys by themselves. The value can be **true** or **false**.
manage_email	No	boolean	Specifies whether to allow IAM users to change their email addresses. The value can be **true** or **false**.
manage_mobile	No	boolean	Specifies whether to allow IAM users to change their mobile numbers. The value can be **true** or **false**.
manage_password	No	boolean	Specifies whether to allow IAM users to change their passwords. The value can be **true** or **false**.

Response Parameters

Status code: 200

Table 5-546 Parameters in the response body

Parameter	Type	Description
protect_policy	protect_policy object	Specifies the operation protection policy.

Table 5-547 protect_policy

Parameter	Type	Description
allow_user	AllowUserBody object	Specifies the attributes IAM users can modify.
operation_protection	boolean	Specifies whether operation protection is enabled. The value can be **true** or **false**.
admin_check	string	Specifies whether a person is designated for verification. If this parameter is set to **on**, a designated person is responsible for verification, and the **scene** parameter is mandatory. If this parameter is set to **off**, the designated operator is responsible for verification.
scene	string	Specifies the verification method. This parameter is mandatory when **admin_check** is set to **on**. The value options are **mobile** and **email**.

Table 5-548 protect_policy.allow_user

Parameter	Type	Description
manage_accesskey	boolean	Specifies whether IAM users are allowed to manage access keys by themselves. The value can be **true** or **false**.
manage_email	boolean	Specifies whether IAM users are allowed to change their email addresses. The value can be **true** or **false**.
manage_mobile	boolean	Specifies whether IAM users are allowed to change their mobile numbers. The value can be **true** or **false**.
manage_password	boolean	Specifies whether IAM users are allowed to change their passwords. The value can be **true** or **false**.

Example Request

Request to enable operation protection

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy

{
  "protect_policy" : {
    "operation_protection" : true
  }
}
```

Example Response

Status code: 200

The request is successful.

```
{
  "protect_policy" : {
    "operation_protection" : false
  }
}
```

Status code: 400

The request body is abnormal.

- Example 1

```
{
  "error_msg" : "'%(key)s' is a required property.",
  "error_code" : "IAM.0072"
}
```

- Example 2

```
{
  "error_msg" : "Invalid input for field '%(key)s'. The value is '%(value)s'.",
  "error_code" : "IAM.0073"
}
```

Status code: 403

Access denied.

- Example 1

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

- Example 2

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
  "error_code" : "IAM.0002"
}
```

Status code: 500

The system is abnormal.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```


Status Codes

Status Code	Description
200	The request is successful.
400	The request body is abnormal.
401	Authentication failed.
403	Access denied.
500	The system is abnormal.

Error Codes

For details, see **Error Codes**.

5.12.2 Querying the Operation Protection Policy

Function

This API is used to query the operation protection policy.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy

Table 5-549 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-550 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Status code: 200

Table 5-551 Parameters in the response body

Parameter	Type	Description
protect_policy	protect_policy object	Specifies the operation protection policy.

Table 5-552 protect_policy

Parameter	Type	Description
allow_user	AllowUserBody object	Specifies the attributes IAM users can modify.
operation_protection	boolean	Specifies whether to enable operation protection. The value can be **true** or **false**.
mobile	string	Specifies the mobile number used for verification. Example:
admin_check	string	Specifies whether a person is designated for verification. If this parameter is set to **on**, you need to specify the **scene** parameter to designate a person for verification. If this parameter is set to **off**, the designated operator is responsible for verification.
email	string	Specifies the email address used for verification. An example value is example@email.com.

Parameter	Type	Description
scene	string	Specifies the verification method. This parameter is mandatory when **admin_check** is set to **on**. The value options are **mobile** and **email**.

Table 5-553 protect_policy.allow_user

Parameter	Type	Description
manage_accesskey	boolean	Specifies whether IAM users are allowed to manage access keys by themselves. The value can be **true** or **false**.
manage_email	boolean	Specifies whether IAM users are allowed to change their email addresses. The value can be **true** or **false**.
manage_mobile	boolean	Specifies whether IAM users are allowed to change their mobile numbers. The value can be **true** or **false**.
manage_password	boolean	Specifies whether IAM users are allowed to change their passwords. The value can be **true** or **false**.

Example Request

Request for querying the operation protection policy

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy
```

Example Response

Status code: 200

The request is successful.

```
{
  "protect_policy" : {
    "operation_protection" : false
  }
}
```

Status code: 403

Access denied.

- Example 1

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
```



```
  "error_code" : "IAM.0002"
}
```

- Example 2

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal server error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.12.3 Modifying the Password Policy

Function

This API is provided for the **administrator** to modify the password policy.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy

Table 5-554 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-555 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-556 Parameter in the request body

Parameter	Mandatory	Type	Description
password_policy	Yes	object	Password policy.

Table 5-557 password_policy

Parameter	Mandatory	Type	Description
maximum_consecutive_identical_chars	No	Integer	Maximum number of times that a character is allowed to consecutively present in a password. Value range: 0–32.
minimum_password_age	No	Integer	Minimum period (minutes) after which users are allowed to make a password change. Value range: 0–1440.

Parameter	Mandatory	Type	Description
minimum_password_length	No	Integer	Minimum number of characters that a password must contain. Value range: 6–32.
number_of_recent_passwords_disallowed	No	Integer	Number of previously used passwords that are not allowed. Value range: 0–10.
password_not_username_or_invert	No	Boolean	Indicates whether the password can be the username or the username spelled backwards.
password_validity_period	No	Integer	Password validity period (days). Value range: 0–180. Value **0** indicates that this requirement does not apply.
password_char_combination	No	Integer	Minimum number of character types that a password must contain. Value range: 2–4.

Response Parameters

Table 5-558 Parameters in the response body

Parameter	Type	Description
password_policy	object	Password policy.

Table 5-559 password_policy

Parameter	Type	Description
maximum_consecutive_identical_chars	Integer	Maximum number of times that a character is allowed to consecutively present in a password.
maximum_password_length	Integer	Maximum number of characters that a password can contain.
minimum_password_age	Integer	Minimum period (minutes) after which users are allowed to make a password change.
minimum_password_length	Integer	Minimum number of characters that a password must contain.

Parameter	Type	Description
number_of_recent_passwords_disallowed	Integer	Number of previously used passwords that are not allowed.
password_not_username_or_invert	Boolean	Indicates whether the password can be the username or the username spelled backwards.
password_requirements	String	Characters that a password must contain.
password_validity_period	Integer	Password validity period (days).
password_char_combination	Integer	Minimum number of character types that a password must contain. Value range: 2–4.

Example Request

Request to change the password policy to the following: Must contain at least 6 characters, at least 3 character types, cannot be the same as the last two passwords, the minimum validity period must be 20 minutes, the password validity period must be 60 days, same characters can be used consecutively for a maximum of three times, and cannot be the same as the user name or the user name spelled backwards

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy

{
  "password_policy" : {
    "minimum_password_length" : 6,
    "number_of_recent_passwords_disallowed" : 2,
    "minimum_password_age" : 20,
    "password_validity_period" : 60,
    "maximum_consecutive_identical_chars" : 3,
    "password_not_username_or_invert" : false,
    "password_char_combination" : 3
  }
}
```

Example Response

Status code: 200

The request is successful.

```
{
  "password_policy" : {
    "password_requirements" : "A password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.",
    "minimum_password_age" : 20,
    "minimum_password_length" : 8,
    "maximum_password_length" : 32,
    "number_of_recent_passwords_disallowed" : 2,
    "password_validity_period" : 60,
    "maximum_consecutive_identical_chars" : 3,
    "password_not_username_or_invert" : true,
```



```
    "password_char_combination" : 3
  }
}
```

Status code: 400

The request body is abnormal.

- Example 1

```
{
  "error_msg" : "'%(key)s' is a required property.",
  "error_code" : "IAM.0072"
}
```

- Example 2

```
{
  "error_msg" : "Invalid input for field '%(key)s'. The value is '%(value)s'.",
  "error_code" : "IAM.0073"
}
```

Status code: 403

Access denied.

- Example 1

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
  "error_code" : "IAM.0002"
}
```

- Example 2

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

Status code: 500

The system is abnormal.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	The request body is abnormal.
401	Authentication failed.
403	Access denied.
500	The system is abnormal.

Error Codes

For details, see **Error Codes**.

5.12.4 Querying the Password Policy of an Account

Function

This API is used to query the password policy of an account.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy

Table 5-560 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-561 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-562 Parameters in the response body

Parameter	Type	Description
password_policy	object	Password policy.

Table 5-563 password_policy

Parameter	Type	Description
maximum_consecutive_identical_chars	Integer	Maximum number of times that a character is allowed to consecutively present in a password.
maximum_password_length	Integer	Maximum number of characters that a password can contain.
minimum_password_age	Integer	Minimum period (minutes) after which users are allowed to make a password change.
minimum_password_length	Integer	Minimum number of characters that a password must contain.
number_of_recent_passwords_disallowed	Integer	Number of previously used passwords that are not allowed.
password_not_username_or_invert	Boolean	Indicates whether the password can be the username or the username spelled backwards.
password_requirements	String	Characters that a password must contain.
password_validity_period	Integer	Password validity period (days).
password_char_combination	Integer	Minimum number of character types that a password must contain. Value range: 2–4.

Example Request

Request for querying the password policy of an account

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy
```

Example Response

Status code: 200

The request is successful.

```
{
  "password_policy" : {
    "password_requirements" : "A password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.",
    "minimum_password_age" : 20,
    "minimum_password_length" : 8,
    "maximum_password_length" : 32,
    "number_of_recent_passwords_disallowed" : 2,
    "password_validity_period" : 60,
    "maximum_consecutive_identical_chars" : 3,
    "password_not_username_or_invert" : true,
    "password_char_combination" : 3
  }
}
```

Status code: 403

Access denied.

- Example 1

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
  "error_code" : "IAM.0002"
}
```

- Example 2

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal server error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.12.5 Modifying the Login Authentication Policy

Function

This API is provided for the **administrator** to modify the login authentication policy.

The API can be called using both the global endpoint and region-specific endpoints. For IAM endpoints, see Regions and Endpoints.

URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy

Table 5-564 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-565 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-566 Parameter in the request body

Parameter	Mandatory	Type	Description
login_policy	Yes	object	Login authentication policy.

Table 5-567 login_policy

Parameter	Mandatory	Type	Description
account_validity_period	No	Integer	Validity period (days) to disable users if they have not logged in within the period. Value range: 0–240.
custom_info_for_login	No	String	Custom information that will be displayed upon successful login.
lockout_duration	No	Integer	Duration (minutes) to lock users out. Value range: 15–30.
login_failed_times	No	Integer	Number of unsuccessful login attempts to lock users out. Value range: 3–10.
period_with_login_failures	No	Integer	Period (minutes) to count the number of unsuccessful login attempts. Value range: 15–60.
session_timeout	No	Integer	Session timeout (minutes) that will apply if you or users created using your account do not perform any operations within a specific period. Value range: 15–1440.
show_recent_login_info	No	Boolean	Indicates whether to display last login information upon successful login. The value can be **true** or **false**.

Response Parameters

Table 5-568 Parameters in the response body

Parameter	Type	Description
login_policy	object	Login authentication policy.

Table 5-569 login_policy

Parameter	Type	Description
account_validity_period	Integer	Validity period (days) to disable users if they have not logged in within the period.

Parameter	Type	Description
custom_info_for_login	String	Custom information that will be displayed upon successful login.
lockout_duration	Integer	Duration (minutes) to lock users out.
login_failed_times	Integer	Number of unsuccessful login attempts to lock users out.
period_with_login_failures	Integer	Period (minutes) to count the number of unsuccessful login attempts.
session_timeout	Integer	Session timeout (minutes) that will apply if you or users created using your account do not perform any operations within a specific period.
show_recent_login_info	Boolean	Indicates whether to display last login information upon successful login.

Example Request

Request for modifying the login authentication policy to the following: The period to count the number of unsuccessful login attempts is 15 minutes, an account that has not been logged in within 99 days will be locked out, the number of login failures within the login duration is 3, the login session expiration time is 16 minutes, and the last login information is displayed.

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy

{
  "login_policy" : {
    "custom_info_for_login" : "",
    "period_with_login_failures" : 15,
    "lockout_duration" : 15,
    "account_validity_period" : 99,
    "login_failed_times" : 3,
    "session_timeout" : 16,
    "show_recent_login_info" : true
  }
}
```

Example Response

Status code: 200

The request is successful.

```
{
  "login_policy" : {
    "custom_info_for_login" : "",
    "period_with_login_failures" : 15,
    "lockout_duration" : 15,
    "account_validity_period" : 99,
    "login_failed_times" : 3,
    "session_timeout" : 16,
    "show_recent_login_info" : true
```



```
  }
}
```

Status code: 400

The request body is abnormal.

- Example 1

```
{
  "error_msg" : "'%(key)s' is a required property.",
  "error_code" : "IAM.0072"
}
```

- Example 2

```
{
  "error_msg" : "Invalid input for field '%(key)s'. The value is '%(value)s'.",
  "error_code" : "IAM.0073"
}
```

Status code: 403

Access denied.

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
  "error_code" : "IAM.0002"
}
```

Status code: 500

The system is abnormal.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	The request body is abnormal.
401	Authentication failed.
403	Access denied.
500	The system is abnormal.

Error Codes

For details, see **Error Codes**.

5.12.6 Querying the Login Authentication Policy

Function

This API is used to query the login authentication policy.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy

Table 5-570 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-571 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-572 Parameters in the response body

Parameter	Type	Description
login_policy	object	Login authentication policy.

Table 5-573 login_policy

Parameter	Type	Description
account_validity_period	Integer	Validity period (days) to disable users if they have not logged in within the period.
custom_info_for_login	String	Custom information that will be displayed upon successful login.
lockout_duration	Integer	Duration (minutes) to lock users out.
login_failed_times	Integer	Number of unsuccessful login attempts to lock users out.
period_with_login_failures	Integer	Period (minutes) to count the number of unsuccessful login attempts.
session_timeout	Integer	Session timeout (minutes) that will apply if you or users created using your account do not perform any operations within a specific period.
show_recent_login_info	Boolean	Indicates whether to display last login information upon successful login.

Example Request

Request to query the login authentication policy

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy
```

Example Response

Status code: 200

The request is successful.

```
{
  "login_policy" : {
    "custom_info_for_login" : "",
    "period_with_login_failures" : 15,
    "lockout_duration" : 15,
    "account_validity_period" : 99,
    "login_failed_times" : 3,
    "session_timeout" : 16,
    "show_recent_login_info" : true
  }
}
```

Status code: 403

Access denied.

- Example 1

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
  "error_code" : "IAM.0002"
}
```


- Example 2

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal server error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.12.7 Modifying the ACL for Console Access

Function

This API is provided for the **administrator** to modify the ACL for console access.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy

Table 5-574 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-575 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-576 Parameter in the request body

Parameter	Mandatory	Type	Description
console_acl_policy	Yes	object	ACL for console access.

Table 5-577 console_acl_policy

Parameter	Mandatory	Type	Description
allow_address_netmasks	No	Array of objects	IPv4 CIDR blocks from which console access is allowed. Specify either **allow_address_netmasks** or **allow_ip_ranges**.
allow_ip_ranges	No	Array of objects	IP address ranges from which console access is allowed. Specify either **allow_address_netmasks** or **allow_ip_ranges**.

Table 5-578 allow_address_netmasks

Parameter	Mandatory	Type	Description
address_netmask	Yes	String	IPv4 CIDR block, for example, **192.168.0.1/24**.
description	No	String	Description about the IPv4 CIDR block.

Table 5-579 allow_ip_ranges

Parameter	Mandatory	Type	Description
description	No	String	Description about an IP address range.
ip_range	Yes	String	IP address range, for example, **0.0.0.0-255.255.255.255**.

Response Parameters

Table 5-580 Parameters in the response body

Parameter	Type	Description
console_acl_policy	object	ACL for console access.

Table 5-581 console_acl_policy

Parameter	Type	Description
allow_address_netmasks	Array of objects	IPv4 CIDR blocks from which console access is allowed.
allow_ip_ranges	Array of objects	IP address ranges from which console access is allowed.

Table 5-582 allow_address_netmasks

Parameter	Type	Description
address_netmask	String	IPv4 CIDR block, for example, **192.168.0.1/24**.
description	String	Description about the IPv4 CIDR block.

Table 5-583 allow_ip_ranges

Parameter	Type	Description
description	String	Description about an IP address range.
ip_range	String	IP address range, for example, **0.0.0.0-255.255.255.255**.

Example Request

Request for modifying the console access policy to only allow console access from IP address range **0.0.0.0-255.255.255.255**

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy

{
  "console_acl_policy" : {
    "allow_ip_ranges" : [ {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : "1"
    }, {
      "ip_range" : "0.0.0.0-255.255.255.253",
      "description" : "12"
    } ],
    "allow_address_netmasks" : [ {
      "address_netmask" : "192.168.0.1/24",
      "description" : "3"
    }, {
      "address_netmask" : "192.168.0.2/23",
      "description" : "4"
    } ]
  }
}
```

Example Response

Status code: 200

The request is successful.

```
{
  "console_acl_policy" : {
    "allow_ip_ranges" : [ {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : ""
    }, {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : ""
    } ],
```



```
  "allow_address_netmasks" : [ {
    "address_netmask" : "192.168.0.1/24",
    "description" : ""
  }, {
    "address_netmask" : "192.168.0.1/24",
    "description" : ""
  } ]
 }
}
```

Status code: 400

The request body is abnormal.

- Example 1

```
{
  "error_msg" : "'%(key)s' is a required property.",
  "error_code" : "IAM.0072"
}
```

- Example 2

```
{
  "error_msg" : "Invalid input for field '%(key)s'. The value is '%(value)s'.",
  "error_code" : "IAM.0073"
}
```

Status code: 500

The system is abnormal.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	The request body is abnormal.
401	Authentication failed.
403	Access denied.
500	The system is abnormal.

Error Codes

For details, see **Error Codes**.

5.12.8 Querying the ACL for Console Access

Function

This API is used to query the ACL for console access.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy

Table 5-584 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-585 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-586 Parameters in the response body

Parameter	Type	Description
console_acl_policy	object	ACL for console access.

Table 5-587 console_acl_policy

Parameter	Type	Description
allow_address_netmasks	Array of objects	IPv4 CIDR blocks from which console access is allowed.

Parameter	Type	Description
allow_ip_ranges	Array of objects	IP address ranges from which console access is allowed.

Table 5-588 allow_address_netmasks

Parameter	Type	Description
address_netmask	String	IPv4 CIDR block, for example, **192.168.0.1/24**.
description	String	Description about the IPv4 CIDR block.

Table 5-589 allow_ip_ranges

Parameter	Type	Description
description	String	Description about an IP address range.
ip_range	String	IP address range, for example, **0.0.0.0-255.255.255.255**.

Example Request

Request for querying the ACL for console access

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy
```

Example Response

Status code: 200

The request is successful.

```
{
  "console_acl_policy" : {
    "allow_ip_ranges" : [ {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : ""
    }, {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : ""
    } ],
    "allow_address_netmasks" : [ {
      "address_netmask" : "192.168.0.1/24",
      "description" : ""
    }, {
      "address_netmask" : "192.168.0.1/24",
      "description" : ""
    } ]
  }
}
```

Status code: 403

Access denied.

- Example 1

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
  "error_code" : "IAM.0002"
}
```

- Example 2

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal server error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.12.9 Modifying the ACL for API Access

Function

This API is provided for the **administrator** to modify the ACL for API access.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy

Table 5-590 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-591 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-592 Parameter in the request body

Parameter	Mandatory	Type	Description
api_acl_policy	Yes	object	ACL for API access.

Table 5-593 api_acl_policy

Parameter	Mandatory	Type	Description
allow_address_netmasks	No	Array of objects	IPv4 CIDR blocks from which API access is allowed. Set either **allow_address_netmasks** or **allow_ip_ranges**.

Parameter	Mandatory	Type	Description
allow_ip_ranges	No	Array of objects	IP address ranges from which API access is allowed. Set either allow_address_netmasks or allow_ip_ranges.

Table 5-594 allow_address_netmasks

Parameter	Mandatory	Type	Description
address_netmask	Yes	String	IPv4 CIDR block, for example, **192.168.0.1/24**.
description	No	String	Description about the IPv4 CIDR block.

Table 5-595 allow_ip_ranges

Parameter	Mandatory	Type	Description
description	No	String	Description about an IP address range.
ip_range	Yes	String	IP address range, for example, **0.0.0.0-255.255.255.255**.

Response Parameters

Table 5-596 Parameters in the response body

Parameter	Type	Description
api_acl_policy	object	ACL for API access.

Table 5-597 api_acl_policy

Parameter	Type	Description
allow_address_netmasks	objects	IPv4 CIDR blocks from which API access is allowed.

Parameter	Type	Description
allow_ip_ranges	objects	IP address ranges from which API access is allowed.

Table 5-598 allow_address_netmasks

Parameter	Type	Description
address_netmask	String	IPv4 CIDR block, for example, **192.168.0.1/24**.
description	String	Description about the IPv4 CIDR block.

Table 5-599 allow_ip_ranges

Parameter	Type	Description
description	String	Description about an IP address range.
ip_range	String	IP address range, for example, **0.0.0.0-255.255.255.255**.

Example Request

Request for modifying the API access policy to only allow API access from IP address range **0.0.0.0-255.255.255.255**

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy

{
  "api_acl_policy" : {
    "allow_ip_ranges" : [ {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : "1"
    }, {
      "ip_range" : "0.0.0.0-255.255.255.253",
      "description" : "12"
    } ],
    "allow_address_netmasks" : [ {
      "address_netmask" : "192.168.0.1/24",
      "description" : "3"
    }, {
      "address_netmask" : "192.168.0.2/23",
      "description" : "4"
    } ]
  }
}
```

Example Response

Status code: 200

The request is successful.

```
{
  "api_acl_policy" : {
    "allow_ip_ranges" : [ {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : ""
    }, {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : ""
    } ],
    "allow_address_netmasks" : [ {
      "address_netmask" : "192.168.0.1/24",
      "description" : ""
    }, {
      "address_netmask" : "192.168.0.1/24",
      "description" : ""
    } ]
  }
}
```

Status code: 400

The request body is abnormal.

- Example 1

```
{
  "error_msg" : "'%(key)s' is a required property.",
  "error_code" : "IAM.0072"
}
```

- Example 2

```
{
  "error_msg" : "Invalid input for field '%(key)s'. The value is '%(value)s'.",
  "error_code" : "IAM.0073"
}
```

Status code: 500

The system is abnormal.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	The request body is abnormal.
401	Authentication failed.
403	Access denied.
500	The system is abnormal.

Error Codes

For details, see **Error Codes**.

5.12.10 Querying the ACL for API Access

Function

This API is used to query the ACL for API access.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy

Table 5-600 URI parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID. For details about how to obtain the account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-601 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-602 Parameters in the response body

Parameter	Type	Description
api_acl_policy	object	ACL for API access.

Table 5-603 api_acl_policy

Parameter	Type	Description
allow_address_netmasks	Array of objects	IPv4 CIDR blocks from which API access is allowed.
allow_ip_ranges	Array of objects	IP address ranges from which API access is allowed.

Table 5-604 allow_address_netmasks

Parameter	Type	Description
address_netmask	String	IPv4 CIDR block, for example, **192.168.0.1/24**.
description	String	Description about the IPv4 CIDR block.

Table 5-605 allow_ip_ranges

Parameter	Type	Description
ip_range	String	IP address range, for example, **0.0.0.0-255.255.255.255**.
description	String	Description about an IP address range.

Example Request

Request for querying the ACL for API access

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy
```

Example Response

Status code: 200

The request is successful.

```
{
  "api_acl_policy" : {
    "allow_ip_ranges" : [ {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : ""
    }, {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : ""
    } ],
    "allow_address_netmasks" : [ {
      "address_netmask" : "192.168.0.1/24",
      "description" : ""
    }, {
      "address_netmask" : "192.168.0.1/24",
```

```
    "description" : ""
  } ]
 }
}
```

Status code: 403

Access denied.

- Example 1

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
  "error_code" : "IAM.0002"
}
```

- Example 2

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

Status code: 404

The requested resource cannot be found.

```
{
 "error_msg" : "Could not find %(target)s: %(target_id)s.",
 "error_code" : "IAM.0004"
}
```

Status code: 500

Internal server error.

```
{
 "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
 "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.12.11 Querying MFA Device Information of IAM Users

Function

This API is provided for the **administrator** to query the MFA device information of IAM users.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-MFA/virtual-mfa-devices

Request Parameters

Table 5-606 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-607 Parameters in the response body

Parameter	Type	Description
virtual_mfa_devices	Array of objects	Virtual MFA device information.

Table 5-608 virtual_mfa_devices

Parameter	Type	Description
serial_number	String	Virtual MFA device serial number.
user_id	String	IAM user ID.

Example Request

Request for querying MFA device information of IAM users

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-MFA/virtual-mfa-devices
```

Example Response

Status code: 200

The request is successful.

```
{
  "virtual_mfa_devices" : [
        {
           "user_id" : "16b26081f43d4c628c4bb88cf32e9...",
           "serial_number" : "iam/mfa/16b26081f43d4c628c4bb88cf32e9..."
         },
        {
           "user_id" : "47026081f43d4c628c4bb88cf32e9...",
           "serial_number" : "iam/mfa/75226081f43d4c628c4bb88cf32e9..."
         }
        ]
}
```

Status code: 403

Access denied.

- Example 1

```
{
   "error_msg" : "You are not authorized to perform the requested action.",
   "error_code" : "IAM.0002"
 }
```

- Example 2

```
{
   "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
   "error_code" : "IAM.0003"
 }
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal server error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.

Status Code	Description
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.12.12 Querying the MFA Device Information of an IAM User

Function

This API can be used by the **administrator** to query the MFA device information of a specified IAM user or used by an IAM user to query their own MFA device information.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-MFA/users/{user_id}/virtual-mfa-device

Table 5-609 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-610 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	If the **administrator** is requesting to query the MFA device information of a specified IAM user, see **Actions**. If an IAM user is requesting to query their own MFA device information, the user token (no special permission requirements) of the user is required.

Response Parameters

Table 5-611 Parameters in the response body

Parameter	Type	Description
virtual_mfa_device	object	Virtual MFA device information.

Table 5-612 virtual_mfa_device

Parameter	Type	Description
serial_number	String	Virtual MFA device serial number.
user_id	String	IAM user ID.

Example Request

Request for querying the MFA device information of an IAM user

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-MFA/users/{user_id}/virtual-mfa-device
```

Example Response

Status code: 200

The request is successful.

```
{
  "virtual_mfa_device" :
    {
      "user_id" : "16b26081f43d4c628c4bb88cf32e9...",
      "serial_number" : "iam/mfa/16b26081f43d4c628c4bb88cf32e9..."
```

```
    }
}
```

Status code: 403

Access denied.

- Example 1

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
  "error_code" : "IAM.0002"
}
```

- Example 2

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal server error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.12.13 Querying Login Protection Configurations of IAM Users

Function

This API is provided for the **administrator** to query the login protection configurations of IAM users.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-USER/login-protects

Request Parameters

Table 5-613 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-614 Parameters in the response body

Parameter	Type	Description
login_protects	Array of objects	Login protection configuration. **NOTE** The response only includes the login protection configurations of users for whom login protection has been enabled.

Table 5-615 login_protects

Parameter	Type	Description
enabled	Boolean	Indicates whether login protection has been enabled for an IAM user. The value can be **true** or **false**.

Parameter	Type	Description
user_id	String	IAM user ID.
verification_method	String	Login authentication method of the IAM user.

Example Request

Request for querying login protection configurations of IAM users

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-USER/login-protects
```

Example Response

Status code: 200

The request is successful.

```
{
  "login_protects" : [
        {
          "user_id" : "75226081f43d4c628c4bb88cf32e9...",
          "enabled" : true,
          "verification_method" : "email"
          },
        {
          "user_id" : "16b26081f43d4c628c4bb88cf32e9...",
          "enabled" : true,
          "verification_method" : "vmfa"
          },
        {
          "user_id" : "56b26081f43d4c628c4bb88cf32e9...",
          "enabled" : true,
          "verification_method" : "sms"
          }
     ]
}
```

NOTE

This API cannot be used to obtain the login protection configurations of users for whom login protection is disabled.

Status code: 403

Access denied.

- Example 1

```
{
  "error_msg" : "You are not authorized to perform the requested action.",
  "error_code" : "IAM.0002"
}
```

- Example 2

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal server error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.12.14 Querying the Login Protection Configuration of an IAM User

Function

This API can be used by the **administrator** to query the login protection configuration of a specified IAM user or used by an IAM user to query their own login protection configuration.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-USER/users/{user_id}/login-protect

Table 5-616 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-617 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	If the **administrator** is requesting to query the login protection configuration of a specified user, see **Actions**. If an IAM user is requesting to query their own login protection configuration, the user token (no special permission requirements) of the user is required.

Response Parameters

Status code: 200

Table 5-618 Parameters in the response body

Parameter	Type	Description
login_protect	object	Login protection configuration.

Table 5-619 login_protect

Parameter	Type	Description
enabled	Boolean	Indicates whether login protection has been enabled for an IAM user. The value can be **true** or **false**.
user_id	String	IAM user ID.

Parameter	Type	Description
verification_method	String	Login authentication method of the IAM user.

Example Request

Request for querying the login protection configuration of an IAM user

```
GET https://iam.myhuaweicloud.eu/v3.0/OS-USER/users/{user_id}/login-protect
```

Example Response

Status code: 200

The request is successful.

```
{
  "login_protect" : {
    "user_id" : "16b26081f43d4c628c4bb88cf32e9...",
    "enabled" : true,
    "verification_method" : "vmfa"
  }
}
```

Status code: 403

Access denied.

- Example 1

```
{
   "error_msg" : "You are not authorized to perform the requested action.",
   "error_code" : "IAM.0002"
 }
```

- Example 2

```
{
   "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
   "error_code" : "IAM.0003"
 }
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "Iam.0004"
}
```

NOTE

This API cannot be used to obtain the login protection configurations of users for whom login protection is disabled, and will return the error code IAM.0004.

Status code: 500

Internal server error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
```



```
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.12.15 Modifying the Login Protection Configuration of an IAM User

Function

This API is provided for the **administrator** to modify the login protection configuration of an IAM user.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-USER/users/{user_id}/login-protect

Table 5-620 URI parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	ID of the IAM user whose login protection configuration is to be modified. For details about how to obtain a user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.

Request Parameters

Table 5-621 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-token	Yes	String	Token with **Security Administrator** permissions.

Table 5-622 Parameter in the request body

Parameter	Mandatory	Type	Description
login_protect	Yes	object	Login protection configuration.

Table 5-623 Login_project

Parameter	Mandatory	Type	Description
enabled	Yes	Boolean	Indicates whether login protection has been enabled for an IAM user. The value can be **true** or **false**.
verification_method	Yes	String	Login authentication method of the IAM user. Options: **sms**, **email**, and **vmfa**.

Response Parameters

Status code: 200

Table 5-624 Parameters in the response body

Parameter	Type	Description
login_protect	object	Login protection configuration.

Table 5-625 login_protect

Parameter	Type	Description
user_id	String	ID of the user whose login protection configuration is to be modified.

Parameter	Type	Description
enabled	Boolean	Whether login protection has been enabled for the user. The value can be **true** or **false**.
verification_method	String	Login authentication method of the IAM user. Options: **sms**, **email**, and **vmfa**.

Example Request

Request for enabling login protection and setting the login authentication method to MFA authentication

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-USER/users/{user_id}/login-protect

{
  "login_protect" : {
    "enabled" : true,
    "verification_method" : "vmfa"
  }
}
```

Example Response

Status code: 200

The request is successful.

```
{
  "login_protect" : {
    "user_id": "16b26081f43d4c628c4bb88cf32e9...",
    "enabled" : true,
    "verification_method" : "vmfa"
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	The request is invalid.
401	Authentication failed.
403	You do not have permission to perform this action.
404	The requested resource cannot be found.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.12.16 Binding a Virtual MFA Device

Function

This API is provided for IAM users to bind a virtual MFA device. Enabling MFA does not affect the validity of the exiting token and MFA authentication cannot be forcibly ignored.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-MFA/mfa-devices/bind

Request Parameters

Table 5-626 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-token	Yes	String	Token (no special permission requirements) of the IAM user corresponding to the **user_id** specified in the request body.

Table 5-627 Parameter in the request body

Parameter	Mandatory	Type	Description
user_id	Yes	String	ID of the user to whom you will bind the virtual MFA device.
serial_number	Yes	String	Serial number of the virtual MFA device.
authentication_code_first	Yes	String	Verification code 1.
authentication_code_second	Yes	String	Verification code 2.

Response Parameters

None

Example Request

Request for binding an MFA device whose serial number is **iam:09f6bd6a96801de40f01c00c85691...:mfa/{device_name}**. The first verification code is **977931**, and the second verification code is **527347**.

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-MFA/mfa-devices/bind

{
  "user_id" : "09f99d8f6a001d4f1f01c00c31968...",
  "authentication_code_first" : "977931",
  "authentication_code_second" : "527347",
  "serial_number" : "iam:09f6bd6a96801de40f01c00c85691...:mfa/{device_name}"
}
```

Example Response

Status code: 204

The request is successful.

Status Codes

Status Code	Description
204	The request is successful.
400	The request is invalid.
401	Authentication failed.
403	You do not have permission to perform this action.
404	The requested resource cannot be found.
409	A conflict occurs when the requested resource is saved.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.12.17 Unbinding a Virtual MFA Device

Function

This API is used by the administrator to unbind a virtual MFA device from an IAM user, or used by an IAM user to unbind their own virtual MFA device.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-MFA/mfa-devices/unbind

Request Parameters

Table 5-628 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	• If the **administrator** is requesting to unbind a virtual MFA device from an IAM user, see **Actions**. • If an IAM user is requesting to unbind their own virtual MFA device, the user token (no special permission requirements) of the user is required.

Table 5-629 Parameter in the request body

Parameter	Mandatory	Type	Description
user_id	Yes	String	ID of the user from whom you will unbind the MFA device.
authentication_code	Yes	String	• **Administrator**: Enter a random 6-digit verification code. • IAM user: Enter the MFA verification code.
serial_number	Yes	String	Serial number of the virtual MFA device.

Response Parameters

None

Example Request

Request for unbinding an MFA device whose serial number is **iam:09f6bd6a96801de40f01c00c85691...:mfa/{device_name}**. The verification code is **373658**.

```
PUT https://iam.myhuaweicloud.eu/v3.0/OS-MFA/mfa-devices/unbind

{
  "user_id" : "09f99d8f6a001d4f1f01c00c31968...",
  "authentication_code" : "373658",
  "serial_number" : "iam:09f6bd6a96801de40f01c00c85691...:mfa/{device_name}"
}
```

Example Response

Status code: 204

The request is successful.

Status Codes

Status Code	Description
204	The request is successful.
400	The request is invalid.
401	Authentication failed.
403	You do not have permission to perform this action.
404	The requested resource cannot be found.
409	A conflict occurs when the requested resource is saved.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.12.18 Creating a Virtual MFA Device

Function

This API is provided for IAM users to create a virtual MFA device.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3.0/OS-MFA/virtual-mfa-devices

Request Parameters

Table 5-630 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token (no special permission requirements) of the IAM user corresponding to the **user_id** specified in the request body.

Table 5-631 Parameter in the request body

Parameter	Mandatory	Type	Description
virtual_mfa_device	Yes	object	MFA device information.

Table 5-632 virtual_mfa_device

Parameter	Mandatory	Type	Description
name	Yes	String	Device name. Minimum length: 1 character Maximum length: 64 characters
user_id	Yes	String	ID of the IAM user for whom you will create the MFA device.

Response Parameters

Status code: 201

Table 5-633 Parameters in the response body

Parameter	Type	Description
virtual_mfa_device	object	Virtual MFA device information.

Table 5-634 virtual_mfa_device

Parameter	Type	Description
serial_number	String	Serial number of the virtual MFA device.
base32_string_seed	String	Base32 seed, which a third-party system can use to generate a CAPTCHA code.

Example Request

Request for creating a virtual MFA device

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-MFA/virtual-mfa-devices

{
  "virtual_mfa_device" : {
    "name" : "{device_name}",
```

```
    "user_id" : "09f99d8f6a001d4f1f01c00c31968..."
  }
}
```

Example Response

Status code: 201

The request is successful.

```
{
  "virtual_mfa_device": {
    "serial_number": "iam:09f6bd6a96801de40f01c00c85691...:mfa/{device_name}",
    "base32_string_seed": "{string}"
  }
}
```

Status Codes

Status Code	Description
201	The request is successful.
400	The request is invalid.
401	Authentication failed.
403	You do not have permission to perform this action.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.12.19 Deleting a Virtual MFA Device

Function

This API is provided for the **administrator** to delete their own virtual MFA device.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3.0/OS-MFA/virtual-mfa-devices

Table 5-635 Query parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	ID of the IAM user whose virtual MFA device is to be deleted, that is, the administrator's user ID. For details about how to obtain the user ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
serial_number	Yes	String	Serial number of the virtual MFA device.

Request Parameters

Table 5-636 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Token with **Security Administrator** permissions of the IAM user specified by **user_id** in the request body.

Response Parameters

None

Example Request

Request for deleting a virtual MFA device

```
DELETE https://iam.myhuaweicloud.eu/v3.0/OS-MFA/virtual-mfa-devices?
user_id=09f6bd85fc801de41f0cc00ce9172...&serial_number=iam:09f6bd6a96801de40f01c00c85691...:mfa/
{device_name}
```

Example Response

Status code: 204

The request is successful.

Status Codes

Status Code	Description
204	The request is successful.
401	Authentication failed.
403	You do not have permission to perform this action.
500	A system error occurred.

Error Codes

For details, see **Error Codes**.

5.13 Federated Identity Authentication Management

5.13.1 Obtaining a Token Through Federated Identity Authentication

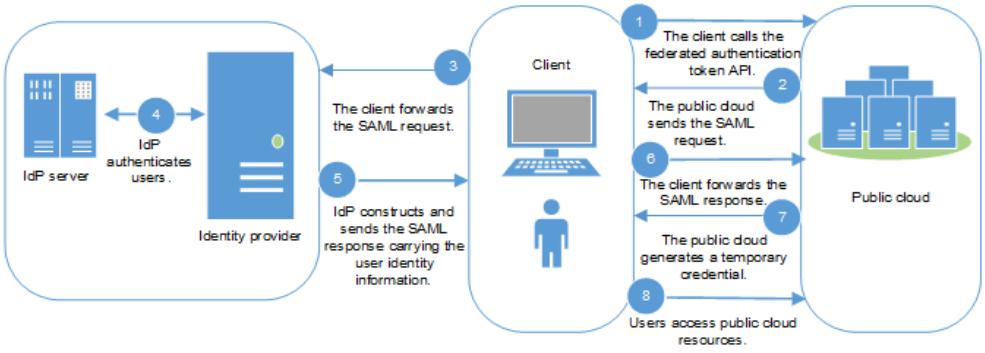
5.13.1.1 SP Initiated

OpenStack and Shibboleth are popular open-source solutions for federated identity authentication. They provide powerful SSO capabilities to connect users to internal and external enterprise applications. This section describes how to use OpenStackClient and Shibboleth ECP Client to obtain a federated authentication token.

Flowchart

The following figure shows the process of SP-initiated federation authentication.

Figure 5-1 Flowchart (SP-initiated)



Description

1. The client calls the API used to obtain a federated token in SP-initiated mode.
2. The cloud platform searches for a metadata file based on the user and IdP information in the URL and sends a SAML request to the client.
3. The client encapsulates the SAML request and forwards the request to the IdP.
4. A user enters a username and password on the IdP server for identity authentication.
5. After authenticating the user, IdP constructs an assertion carrying the user identity information and sends a SAML response to the client.
6. The client encapsulates the SAML response and forwards the response to the cloud platform.
7. The cloud platform verifies and authenticates the assertion, and generates a temporary access credential according to the identity conversion rules of the user configured for the identity provider.
8. The user can access public cloud resources based on assigned permissions.

OpenStackClient

OpenStackClient is a command-line client that can be installed only by a user with root permissions. Configuration of this client requires only common user permissions.

NOTICE

Call APIs in a secure network environment (in a VPN or cloud server). Otherwise, you may encounter man-in-the-middle (MITM) attacks.

Step 1 Create an environment variable file in the installation directory of OpenStackClient, and add the username, password, region, SAML protocol version, and IAM address in the file. **Table 5-637** describes the parameters.

For example:

export OS_IDENTITY_API_VERSION=3

export OS_AUTH_TYPE=v3samlpassword

export OS_AUTH_URL=https://example:443/v3

export OS_IDENTITY_PROVIDER=idpid

export OS_PROTOCOL=saml

export OS_IDENTITY_PROVIDER_URL=https://idp.example.com/idp/profile/SAML2/SOAP/ECP

export OS_USERNAME=username

export OS_PASSWORD=userpassword

export OS_DOMAIN_NAME=example-domain-name

Table 5-637 Parameter description

Parameter	Description
OS_IDENTITY_API_VERSION	Authentication API version. The value is fixed at **3**.
OS_AUTH_TYPE	Authentication type. The value is fixed at **v3samlpassword**.
OS_AUTH_URL	Authentication URL. The value format is **https://***IAM _address*:*Port_number*/*API_version*. • *Port_number* is fixed at **443**. • *API_version* is fixed at **v3**.
OS_IDENTITY_PROVIDER	Name of an identity provider created on the cloud platform. For example: **Publiccloud-Shibboleth**.
OS_DOMAIN_NAME	Name of the account to be authenticated
OS_PROTOCOL	SAML protocol version. The value is fixed at **saml**.
OS_IDENTITY_PROVIDER_URL	URL of the identity provider used to handle the authentication requests initiated by ECP
OS_USERNAME	Name of a user authenticated using the identity provider
OS_PASSWORD	Password of the user

Step 2 Run the following command to set environment variables:

source keystonerc

Step 3 Run the following command to obtain a token:

openstack token issue

```
>>openstack token issue
command: token issue -> openstackclient.identity.v3.token.IssueToken (auth=True)
Using auth plugin: v3samlpassword
+------------------------------------------------------------------------------------------------------------
| Field   | Value
| expires | 2018-04-16T03:46:51+0000
| id      | MIIDbQYJKoZIhvcNAQcCoIIDXjXXX...
| user_id | 9B7CJy5ME14f0fQKhb6HJVQdpXXX...
```

In the command output, **id** is the obtained federated authentication token.

----End

Shibboleth ECP Client

Step 1 Configure the **metadata-providers.xml** files in Shibboleth IdP v3 and place them in the corresponding path.


```
<MetadataProvider id="LocalMetadata1"xsi:type="FilesystemMetadataProvider" metadataFile="C:\Program Files (x86)\Shibboleth\IdP\metadata\web_metadata.xml"/>
<MetadataProvider id="LocalMetadata2"xsi:type="FilesystemMetadataProvider" metadataFile="C:\Program Files (x86)\Shibboleth\IdP\metadata\api_metadata.xml"/>
```

NOTE

- **MetadataProvider id** indicates the name of the downloaded metadata file of the SP system.
- **metadataFile** indicates the path for storing the metadata file of the SP system in the IdP system.

Step 2 Configure the **attribute-filter.xml** file in Shibboleth IdP v3.

```
<afp:AttributeFilterPolicy id="example1">
    <afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="https://auth.example.com/" />
    <afp:AttributeRule attributeID="eduPersonPrincipalName">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
    <afp:AttributeRule attributeID="uid">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
    <afp:AttributeRule attributeID="mail">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
</afp:AttributeFilterPolicy>

<afp:AttributeFilterPolicy id="example2">
    <afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="https://iam.{region_id}.example.com" />
    <afp:AttributeRule attributeID="eduPersonPrincipalName">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
    <afp:AttributeRule attributeID="uid">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
    <afp:AttributeRule attributeID="mail">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

NOTE

AttributeFilterPolicy id indicates the name of the downloaded metadata file of the SP system.

value indicates the **EntityID** in the metadata file of the SP system.

Step 3 Configure the endpoint of the IdP system in the **ecp.py** script.

```
# mapping from user friendly names or tags to IdP ECP enpoints
IDP_ENDPOINTS = {
    "idp1": "https://idp.example.com/idp/profile/SAML2/SOAP/ECP"
}
```

Step 4 Run the **ecp.py** script to obtain a federated authentication token.

```
>>python ecp.py
Usage: ecp.py [options] IdP_tag target_url login
>>python ecp.py -d idp1 https://iam.{region_id}.example.com/v3/OS-FEDERATION/identity_providers/idp_example/protocols/saml/auth {username}
X-Subject-Token: MIIDbQYJKoZIhvcNAQcCoIIDXXX...
```

X-Subject-Token is the obtained federated authentication token.

----End

5.13.1.2 IdP Initiated

This section uses the **Client4ShibbolethIdP** script as an example to describe how to obtain a federated authentication token in the IdP-initiated mode. The **Client4ShibbolethIdP** script simulates a user logging in to an IdP system using a browser, helping you to develop your own IdP client script.

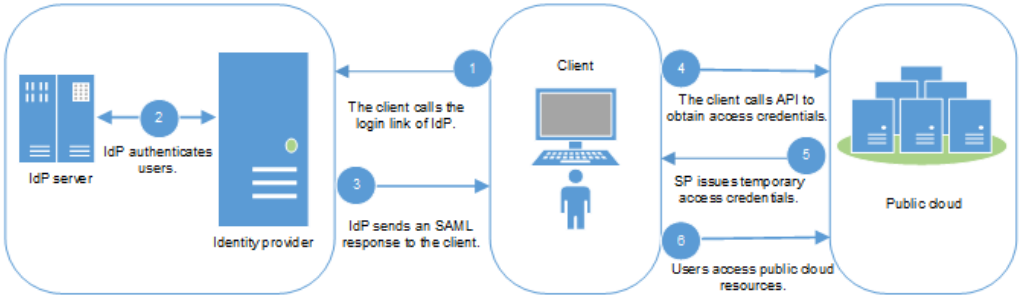
Prerequisites

- Your IdP server supports IdP-initiated federated identity authentication.
- The Python library **BeautifulSoup 4** has been installed on the client.

Flowchart

The following figure shows the process of IdP-initiated federation authentication.

Figure 5-2 Flowchart (IdP-initiated)



Description

1. The client visits the login link provided by IdP for IdP-initiated login and sets the public cloud address (**entityID** in the metadata file of the cloud system) in the login link.
2. The client displays the IdP login page, allowing users to submit identity information to IdP for authentication.
3. After authenticating the user, IdP constructs an assertion carrying the user identity information and sends a SAML response to the client.
4. The client encapsulates the SAML response and forwards it to the cloud system to call the API used to obtain a federated token in the IdP-initiated mode.
5. The cloud system verifies and authenticates the assertion, and generates a temporary access credential according to the identity conversion rules of the user configured for the identity provider.
6. The user can access public cloud resources based on assigned permissions.

Implementation on the Client

This section uses the **Client4ShibbolethIdP.py** script to describe how to implement federated identity authentication for API/CLI access to the cloud system from an IdP.

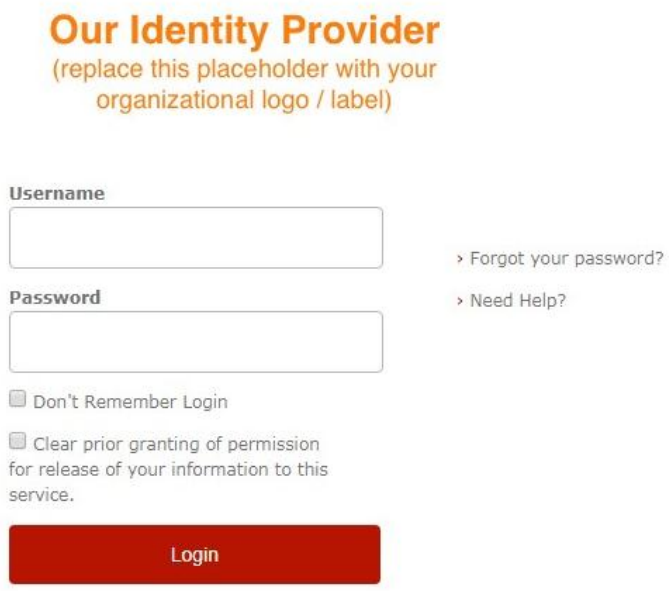
Step 1 Configure the login URL of the IdP.

Table 5-638 Login URLs of common IdP products

IdP	SP Parameter in URL	Example Login URL
ADFS	logintorp	https://adfs-server.contoso.com/adfs/ls/IdpInitiatedSignon.aspx?logintorp=https://iam.example.com
Shibboleth	providerId	https://idp.example.org/idp/profile/SAML2/Unsolicited/SSO?providerId=iam.example.com
SimpleSAMLphp	spentityid	https://idp.example.org/simplesaml/saml2/idp/SSOService.php?spentityid=iam.example.com

After the configuration, enter a login URL in the address bar of a browser. The following page is displayed.

Figure 5-3 Login page



Client4ShibbolethIdP script:

```
import sys
import requests
import getpass
import re
from bs4 import BeautifulSoup
from urlparse import urlparse

# SSL certificate verification: Whether or not strict certificate
# verification is done, False should only be used for dev/test
sslverification = True

# Get the federated credentials from the user
```

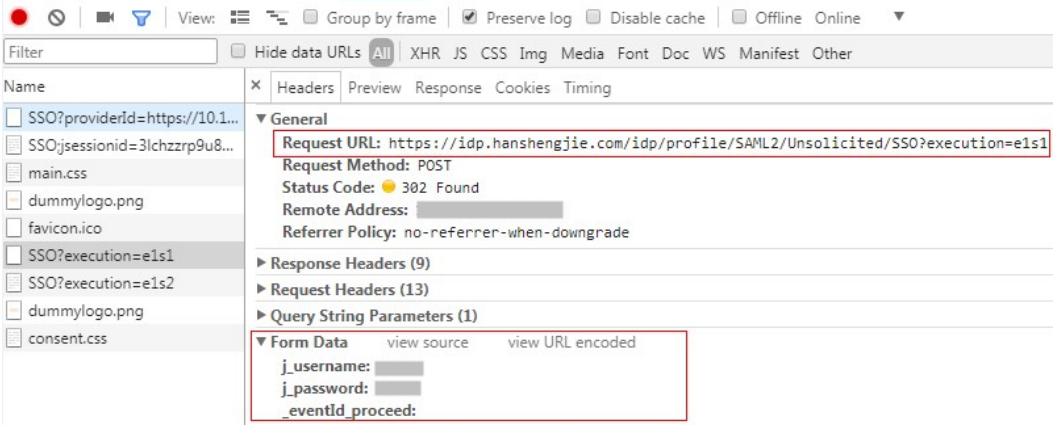


```
print "Username:",
username = raw_input()
password = getpass.getpass()
print ''

session = requests.Session()

# The initial url that starts the authentication process.
idp_entry_url = 'https://idp.example.com/idp/profile/SAML2/Unsolicited/SSO?providerId=https://
iam.example.com'

# Programmatically get the SAML assertion,open the initial IdP url# and follows all of the HTTP302
redirects, and gets the resulting# login page
formresponse = session.get(idp_entry_url, verify=sslverification)
# Capture the idp_authform_submit_url,which is the final url after# all the 302s
idp_authform_submit_url = formresponse.url
```

Step 2 The client uses Beautifulsoup 4 to capture the user information and requested action, and then constructs and sends an identity authentication request to the IdP.

The client acquires all form data submitted through the login page.

Figure 5-4 Authentication information (1)



Client4ShibbolethIdP script:

```
# Parse the response and extract all the necessary values in order to build a dictionary of all of the form
values the IdP expects
formsoup = BeautifulSoup(formresponse.text.decode('utf8'), "lxml")
payload = {}

for inputtag in formsoup.find_all(re.compile('(INPUT|input)')):
    name = inputtag.get('name', '')
    value = inputtag.get('value', '')
    if "username" in name.lower():
        payload[name] = username
    elif "password" in name.lower():
        payload[name] = password
    else:
        payload[name] = value

for inputtag in formsoup.find_all(re.compile('(FORM|form)')):
    action = inputtag.get('action')
    if action:
        parsedurl = urlparse(idp_entry_url)
        idp_authform_submit_url = parsedurl.scheme + "://" + parsedurl.netloc + action
```

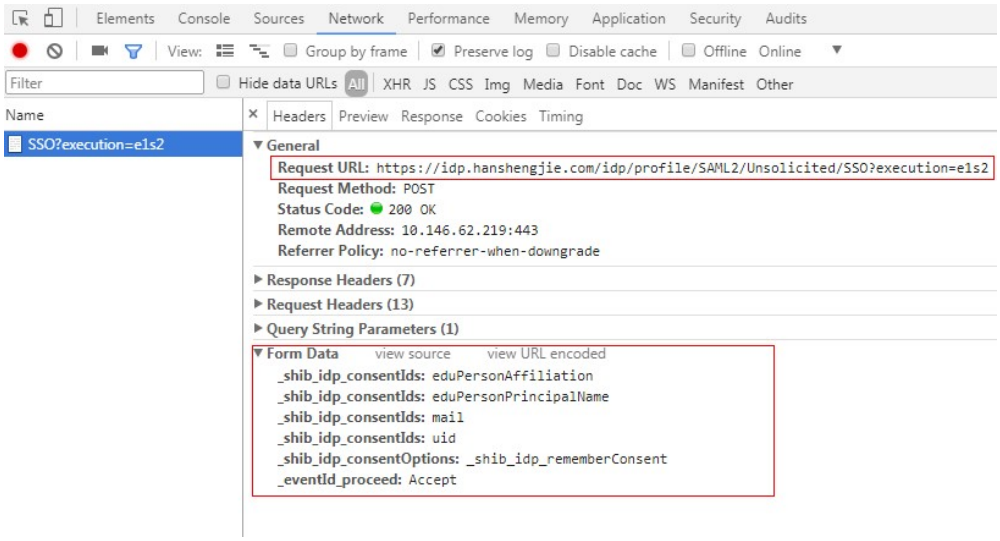


```
# please test on browser first, add other parameters in payload
payload["_eventId_proceed"] = ""

formresponse = session.post(
    idp_authform_submit_url, data=payload, verify=sslverification)
```

Step 3 The client parses the next page. (Some IdPs display a user attribute page.)

The client acquires all form data submitted through the login page.

Figure 5-5 Authentication information (2)



Client4ShibbolethIdP script:

```
# In shebbleth IdP v3, browser will show attributes page for user,# so we need parse the page
formsoup = BeautifulSoup(formresponse.text.decode('utf8'), "lxml")
payload = {}

# Add other form data required from browser to payload
_shib_idp_consentIds = []
for inputtag in formsoup.find_all(re.compile('input')):
    name = inputtag.get("name")
    value = inputtag.get("value")
    if name == "_shib_idp_consentIds":
        _shib_idp_consentIds.append(value)
payload["_shib_idp_consentIds"] = _shib_idp_consentIds
payload["_shib_idp_consentOptions"] = "_shib_idp_rememberConsent"
payload["_eventId_proceed"] = "Accept"

# user can get the action url from the html file
nexturl = "https://idp.example.com/idp/profile/SAML2/Unsolicited/SSO?execution=e1s2"

for inputtag in formsoup.find_all(re.compile('(FORM|form)')):
    action = inputtag.get('action')
    if action:
        parsedurl = urlparse(idp_entry_url)
        nexturl = parsedurl.scheme + "://" + parsedurl.netloc + action

response = session.post(
    nexturl, data=payload, verify=sslverification)
```

Step 4 If the authentication is successful, the client parses the SAML response sent by the IdP.

Client4ShibbolethIdP script:


```
# Decode the response and extract the SAML assertion
soup = BeautifulSoup(response.text.decode('utf8'), "lxml")
SAMLResponse = ''

# Look for the SAMLResponse attribute of the input tag
for inputtag in soup.find_all('input'):
    if (inputtag.get('name') == 'SAMLResponse'):
        SAMLResponse = inputtag.get('value')

# Better error handling is required for production use.
if (SAMLResponse == ''):
    print 'Response did not contain a valid SAML assertion, please troubleshooting in Idp side.'
    sys.exit(0)
```

Step 5 Obtain an unscoped token. For details, see **Obtaining an Unscoped Token (IdP Initiated)**.

Client4ShibbolethIdP script:

```
# Set headers
headers = {}
headers["X-Idp-Id"] = "test_local_idp"

# IAM API url: get unscoped token on IDP initiated mode
sp_unscoped_token_url = "https://iam.example.com/v3.0/OS-FEDERATION/tokens"

# Set form data
payload = {}
payload["SAMLResponse"] = SAMLResponse
response = session.post(
    sp_unscoped_token_url, data=payload, headers=headers, verify=sslverification)

# Debug only
print(response.text)
print "Status Code: " + str(response.status_code)
if response.status_code != 201:
    sys.exit(1)

unscoped_token = response.headers.get("X-Subject-Token") if "X-Subject-Token" in response.headers.keys()
else None
if unscoped_token:
    print ">>>>>>>X-Subject-Token: " + unscoped_token
```

Step 6 Obtain a scoped token. For details, see **Obtaining a Scoped Token**.

Client4ShibbolethIdP script:

```
payload = {
    "auth": {
        "identity": {
            "methods": ["token"],
            "token": {
                "id": unscoped_token
            }
        },
        "scope": {
            "project": {
                "name": "{region_id}_test1"
            }
        }
    }
}

sp_scoped_token_url = "https://10.120.171.90:31943/v3/auth/tokens"

response = session.post(
    sp_scoped_token_url, json=payload, verify=sslverification)

# Debug only
```



```
print "Status Code: " + str(response.status_code)
if response.status_code != 201:
    print response.text
    sys.exit(1)

scoped_token = response.text if response.status_code == 201 else None
if scoped_token:
    print ">>>>>>Scoped Token:" + scoped_token
```

Step 7 Obtain a temporary access key. For details, see **Obtaining a Temporary Access Key and Security Token Through a Token**.

Client4ShibbolethIdP script:

```
# Set form data
payload = {
    "auth": {
        "identity": {
            "methods": ["token"],
            "token": {
                "duration_seconds": "900"
            }
        }
    }
}

# Set headers
headers = {}
headers["X-Auth-Token"] = unscoped_token

sp_STS_token_url = "https://10.120.171.90:31943/v3.0/OS-CREDENTIAL/securitytokens"

response = session.post(
    sp_STS_token_url, json=payload, headers=headers, verify=sslverification)

# Debug only
print "Status Code: " + str(response.status_code)
if response.status_code != 201:
    print response.text
    sys.exit(1)

sts_token = response.text if response.status_code == 201 else None
if sts_token:
    print ">>>>>>STS Token:" + sts_token
```

----End

5.13.2 Identity Providers

5.13.2.1 Listing Identity Providers

Function

This API is used to list all identity providers.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/OS-FEDERATION/identity_providers

Request Parameters

Table 5-639 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-640 Parameters in the response body

Parameter	Type	Description
identity_providers	Array of objects	Identity provider information.
links	Object	Resource link information.

Table 5-641 identity_providers

Parameter	Type	Description
sso_type	string	Identity provider type. The following two types are supported: • **virtual_user_sso**: The user is mapped to a virtual user after the federated login is redirected. • **iam_user_sso**: The user is mapped to an IAM user after the federated login is redirected. The default value is **virtual_user_sso**.
id	String	Identity provider ID.
description	String	Description of the identity provider.
enabled	Boolean	Enabling status of the identity provider. **true** indicates that the identity provider is enabled. **false** indicates that the identity provider is disabled. The default value is **false**.

Parameter	Type	Description
remote_ids	Array of strings	List of federated user IDs configured for the identity provider.
links	Object	Identity provider resource link.

Table 5-642 identity_providers.links

Parameter	Type	Description
self	String	Identity provider resource link.
protocols	String	Protocol resource link.

Table 5-643 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying identity providers

```
GET https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers
```

Example Response

Status code: 200

The request is successful.

```
{
    "links": {
        "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers",
        "previous": null,
        "next": null
    },
    "identity_providers": [
        {
            "remote_ids": [],
            "enabled": true,
            "id": "ACME",
            "sso_type": "iam_user_sso",
            "links": {
                "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME",
                "protocols": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME/
protocols"
            },
            "description": "Stores ACME identities."
```

```
    }
  ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.2.2 Querying Identity Provider Details

Function

This API is used to query the details about an identity provider.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/OS-FEDERATION/identity_providers/{id}

Table 5-644 URI parameters

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the identity provider to be queried.

Request Parameters

Table 5-645 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token (no special permission requirements).

Response Parameters

Table 5-646 Parameters in the response body

Parameter	Type	Description
identity_provider	Object	Identity provider information.

Table 5-647 identity_provider

Parameter	Type	Description
sso_type	string	Identity provider type. The following two types are supported: • **virtual_user_sso**: The federated user is mapped to a virtual user after the login is redirected. • **iam_user_sso**: The federated user is mapped to an IAM user after the login is redirected. The default value is **virtual_user_sso**.
id	String	Identity provider ID.
description	String	Description of the identity provider.
enabled	Boolean	Enabling status of the identity provider. **true** indicates that the identity provider is enabled. **false** indicates that the identity provider is disabled. The default value is **false**.
remote_ids	Array of strings	List of federated user IDs configured for the identity provider.
links	Object	Identity provider resource link.

Table 5-648 identity_provider.links

Parameter	Type	Description
self	String	Identity provider resource link.
protocols	String	Protocol resource link.

Example Request

Request for querying identity provider details

```
GET https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "identity_provider": {
        "remote_ids": [],
        "enabled": true,
        "id": "ACME",
        "sso_type": "iam_user_sso",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME",
            "protocols": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME/
protocols"
        },
        "description": "Stores ACME identities."
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.2.3 Creating an Identity Provider

Function

This API is provided for the **administrator** to create an identity provider. After creating an identity provider, register a protocol and modify the identity provider configuration.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3/OS-FEDERATION/identity_providers/{id}

Table 5-649 URI parameters

Parameter	Mandatory	Type	Description
id	Yes	String	Identity provider name.

Request Parameters

Table 5-650 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-651 Parameters in the request body

Parameter	Mandatory	Type	Description
identity_provider	Yes	Object	Identity provider information.

Table 5-652 identity_provider

Parameter	Mandatory	Type	Description
sso_type	No	string	Identity provider type. The following two types are supported: • **virtual_user_sso**: The federated user is mapped to a virtual user after the login is redirected. • **iam_user_sso**: The federated user is mapped to an IAM user after the login is redirected. If you select this type, ensure that you have created an IAM user on Huawei Cloud. The default value is **virtual_user_sso**.
description	No	String	Description of the identity provider.
enabled	No	Boolean	Enabling status of the identity provider. **true** indicates that the identity provider is enabled. **false** indicates that the identity provider is disabled. The default value is **false**.

Response Parameters

Table 5-653 Parameters in the response body

Parameter	Type	Description
identity_provider	Object	Identity provider information.

Table 5-654 identity_provider

Parameter	Type	Description
sso_type	string	Identity provider type.
id	String	Identity provider ID.
description	String	Description of the identity provider.
enabled	Boolean	Enabling status of the identity provider. **true** indicates that the identity provider is enabled. **false** indicates that the identity provider is disabled. The default value is **false**.

Parameter	Type	Description
remote_ids	Array of strings	List of federated user IDs configured for the identity provider.
links	Object	Identity provider resource link.

Table 5-655 identity_provider.links

Parameter	Type	Description
self	String	Identity provider resource link.
protocols	String	Protocol resource link.

Example Request

Request for creating an identity provider and enable it

```
PUT https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{id}
{
    "identity_provider": {
        "description": "Stores ACME identities.",
        "enabled": true
    }
}
```

Example Response

Status code: 201

The request is successful.

```
{
    "identity_provider": {
        "remote_ids": [],
        "enabled": true,
        "id": "ACME",
        "sso_type": "iam_user_sso",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME",
            "protocols": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME/
protocols"
        },
        "description": "Stores ACME identities."
    }
}
```

Status Codes

Status Code	Description
201	The request is successful.
400	Invalid parameters.

Status Code	Description
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
409	A resource conflict occurs.
413	The request entity is too large.
500	The request entity is too large.
503	Service unavailable.

Error Codes

None

5.13.2.4 Modifying a SAML Identity Provider

Function

This API is provided for the **administrator** to modify a SAML identity provider.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PATCH /v3/OS-FEDERATION/identity_providers/{id}

Table 5-656 URI parameters

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the identity provider to be updated.

Request Parameters

Table 5-657 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-658 Parameters in the request body

Parameter	Mandatory	Type	Description
identity_provider	Yes	Object	Identity provider information.

Table 5-659 identity_provider

Parameter	Mandatory	Type	Description
description	No	String	Description of the identity provider.
enabled	No	Boolean	Enabling status of the identity provider. **true** indicates that the identity provider is enabled. **false** indicates that the identity provider is disabled. The default value is **false**.

Response Parameters

Table 5-660 Parameters in the response body

Parameter	Type	Description
identity_provider	Object	Identity provider information.

Table 5-661 identity_provider

Parameter	Type	Description
sso_type	string	Identity provider type.
id	String	Identity provider ID.
description	String	Description of the identity provider.
enabled	Boolean	Enabling status of the identity provider. **true** indicates that the identity provider is enabled. **false** indicates that the identity provider is disabled. The default value is **false**.
remote_ids	Array of strings	List of federated user IDs configured for the identity provider.
links	Object	Identity provider resource link.

Table 5-662 identity_provider.links

Parameter	Type	Description
self	String	Identity provider resource link.
protocols	String	Protocol resource link.

Example Request

Request for disabling the SAML identity provider

```
PATCH https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{id}
{
    "identity_provider": {
        "description": "Stores ACME identities.",
        "enabled": false
    }
}
```

Example Response

Status code: 200

The request is successful.

```
{
    "identity_provider": {
        "remote_ids": [],
        "enabled": false,
        "id": "ACME",
        "sso_type": "iam_user_sso",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME",
            "protocols": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME/
protocols"
        },
        "description": "Stores ACME identities."
```



```
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
409	A resource conflict occurs.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.2.5 Deleting a SAML Identity Provider

Function

This API is provided for the **administrator** to delete a SAML identity provider.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3/OS-FEDERATION/identity_providers/{id}

Table 5-663 URI parameters

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the identity provider to be deleted.

Request Parameters

Table 5-664 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for deleting a SAML identity provider

```
DELETE https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{id}
```

Example Response

None

Status Codes

Status Code	Description
204	The identity provider is deleted successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.2.6 Creating an OpenID Connect Identity Provider Configuration

Function

This API is provided for the **administrator** to create an OpenID Connect identity provider configuration after **creating an identity provider** and **registering a protocol (OpenID Connect)**.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config

Table 5-665 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider name.

Request Parameters

Table 5-666 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-667 Parameter in the request body

Parameter	Mandatory	Type	Description
openid_connect_config	Yes	object	OpenID Connect configurations.

Table 5-668 CreateOpenIDConnectConfig

Parameter	Mandatory	Type	Description
access_mode	Yes	String	Access type. Options: • **program_console**: programmatic access and management console access. • **program**: programmatic access only.
idp_url	Yes	String	URL of the OpenID Connect identity provider. This field corresponds to the **iss** field in the ID token. Length: 10 to 255 characters
client_id	Yes	String	ID of a client registered with the OpenID Connect identity provider. Length: 5 to 255 characters
authorization_endpoint	No	String	Authorization endpoint of the OpenID Connect identity provider. This field is required only if the access type is set to programmatic access and management console access. Length: 10 to 255 characters

Parameter	Mandatory	Type	Description
scope	No	String	Scopes of authorization requests. This field is required only if the access type is set to programmatic access and management console access. Enumerated values: • openid • email • profile **NOTE** • **openid** must be specified for this field. • Specify 1 to 10 values, and separate them with spaces. Example: **openid**, **openid email**, **openid profile**, and **openid email profile**.
response_type	No	String	Response type. This field is required only if the access type is set to programmatic access and management console access. Enumerated value: • id_token
response_mode	No	String	Response mode. This field is required only if the access type is set to programmatic access and management console access. Enumerated values: • fragment • form_post

signing_key	Yes	String	Public key used to sign the ID token of the OpenID Connect identity provider.
			Length: 10 to 30,000 characters
			Format example:
			{
			"keys":[
			{
			"kid":"d05ef20c4512645vv1..." ,
			"n":"cws_cnjiwsbvweolwn_-vnl...",
			"e":"AQAB",
			"kty":"RSA",
			"use":"sig",
			"alg":"RS256"
			}
			]
			}

Response Parameters

Status code: 201

Table 5-669 Parameters in the response body

Parameter	Type	Description
openid_connect_config	object	OpenID Connect configurations.

Table 5-670 openid_connect_config

Parameter	Type	Description
access_mode	String	Access type. Options: • **program_console**: programmatic access and management console access. • **program**: programmatic access only.
idp_url	String	URL of the OpenID Connect identity provider. This field corresponds to the **iss** field in the ID token.
client_id	String	ID of a client registered with the OpenID Connect identity provider.
authorization_endpoint	String	Authorization endpoint of the OpenID Connect identity provider. This field is required only if the access type is set to programmatic access and management console access.
scope	String	Scopes of authorization requests. This field is required only if the access type is set to programmatic access and management console access. Enumerated values: • openid • email • profile **NOTE** • **openid** must be specified for this field. • Specify 1 to 10 values, and separate them with spaces. Example: **openid**, **openid email**, **openid profile**, and **openid email profile**.

Parameter	Type	Description
response_type	String	Response type. This field is required only if the access type is set to programmatic access and management console access. Enumerated value: • id_token
response_mode	String	Response mode. This field is required only if the access type is set to programmatic access and management console access. Enumerated values: • fragment • form_post
signing_key	String	Public key used to sign the ID token of the OpenID Connect identity provider.

Example Request

- Request for creating an OpenID Connect identity provider that supports programmatic access configurations

```
POST /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config

{
  "openid_connect_config" : {
    "access_mode" : "program",
    "idp_url" : "https://accounts.example.com",
    "client_id" : "client_id_example",
    "signing_key" : "{\"keys\":[{\"kty\":\"RSA\",\"e\":\"AQAB\",\"use\":\"sig\",\"n\":\"example\",\"kid
\":\"kid_example\",\"alg\":\"RS256\"}]}"
  }
}
```

- Request for creating an OpenID Connect identity provider that supports programmatic access and console access configurations

```
POST /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config

{
  "openid_connect_config" : {
    "access_mode" : "program_console",
    "idp_url" : "https://accounts.example.com",
    "client_id" : "client_id_example",
    "authorization_endpoint" : "https://accounts.example.com/o/oauth2/v2/auth",
    "scope" : "openid",
    "response_type" : "id_token",
    "response_mode" : "form_post",
    "signing_key" : "{\"keys\":[{\"kty\":\"RSA\",\"e\":\"AQAB\",\"use\":\"sig\",\"n\":\"example\",\"kid
\":\"kid_example\",\"alg\":\"RS256\"}]}"
  }
}
```

Example Response

Status code: 201

The identity provider is created successfully.

- Example 1

```
{
  "openid_connect_config" : {
    "access_mode" : "program",
    "idp_url" : "https://accounts.example.com",
    "client_id" : "client_id_example",
    "signing_key" : "{\"keys\":[{\"kty\":\"RSA\",\"e\":\"AQAB\",\"use\":\"sig\",\"n\":\"example\",\"kid
\":\"kid_example\",\"alg\":\"RS256\"}]}"
  }
}
```

- Example 2

```
{
  "openid_connect_config" : {
    "access_mode" : "program_console",
    "idp_url" : "https://accounts.example.com",
    "client_id" : "client_id_example",
    "authorization_endpoint" : "https://accounts.example.com/o/oauth2/v2/auth",
    "scope" : "openid",
    "response_type" : "id_token",
    "response_mode" : "form_post",
    "signing_key" : "{\"keys\":[{\"kty\":\"RSA\",\"e\":\"AQAB\",\"use\":\"sig\",\"n\":\"example\",\"kid
\":\"kid_example\",\"alg\":\"RS256\"}]}"
  }
}
```

Status Codes

Status Code	Description
201	The identity provider is created successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
409	The resource already exists.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.13.2.7 Modifying an OpenID Connect Identity Provider

Function

This API is provided for the **administrator** to modify an OpenID Connect identity provider.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config

Table 5-671 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider ID. Length: 1 to 64 characters

Request Parameters

Table 5-672 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-673 Parameter in the request body

Parameter	Mandatory	Type	Description
openid_connect_config	Yes	object	OpenID Connect configurations.

Table 5-674 openid_connect_config

Parameter	Mandatory	Type	Description
access_mode	No	String	Access type. Options: • **program_console**: programmatic access and management console access. • **program**: programmatic access only.
idp_url	No	String	URL of the OpenID Connect identity provider. This field corresponds to the **iss** field in the ID token. Length: 10 to 255 characters
client_id	No	String	ID of a client registered with the OpenID Connect identity provider. Length: 5 to 255 characters
authorization_endpoint	No	String	Authorization endpoint of the OpenID Connect identity provider. This field is required only if the access type is set to programmatic access and management console access. Length: 10 to 255 characters
scope	No	String	Scopes of authorization requests. This field is required only if the access type is set to programmatic access and management console access. Enumerated values: • openid • email • profile **NOTE** • **openid** must be specified for this field. • Specify 1 to 10 values, and separate them with spaces. Example: **openid**, **openid email**, **openid profile**, and **openid email profile**.

Parameter	Mandatory	Type	Description
response_type	No	String	Response type. This field is required only if the access type is set to programmatic access and management console access. Enumerated value: • id_token
response_mode	No	String	Response mode. This field is required only if the access type is set to programmatic access and management console access. Enumerated values: • fragment • form_post

signing_key	No	String	Public key used to sign the ID token of the OpenID Connect identity provider.
			Length: 10 to 30,000 characters
			Format example:
			{
			"keys":[
			{
			"kid":"d05ef20c4512645vv1..." ,
			"n":"cws_cnjiwsbvweolwn_-vnl...",
			"e":"AQAB",
			"kty":"RSA",
			"use":"sig",
			"alg":"RS256"
			}
			]
			}

Response Parameters

Status code: 200

Table 5-675 Parameters in the response body

Parameter	Type	Description
openid_connect_config	object	OpenID Connect configurations.

Table 5-676 OpenIDConnectConfig

Parameter	Type	Description
access_mode	String	Access type. Options: • **program_console**: programmatic access and management console access. • **program**: programmatic access only.
idp_url	String	URL of the OpenID Connect identity provider. This field corresponds to the **iss** field in the ID token.
client_id	String	ID of a client registered with the OpenID Connect identity provider.
authorization_endpoint	String	Authorization endpoint of the OpenID Connect identity provider. This field is required only if the access type is set to programmatic access and management console access.
scope	String	Scopes of authorization requests. This field is required only if the access type is set to programmatic access and management console access. Enumerated values: • openid • email • profile **NOTE** • **openid** must be specified for this field. • Specify 1 to 10 values, and separate them with spaces. Example: **openid**, **openid email**, **openid profile**, and **openid email profile**.
response_type	String	Response type. This field is required only if the access type is set to programmatic access and management console access. Enumerated value: • id_token

Parameter	Type	Description
response_mode	String	Response mode. This field is required only if the access type is set to programmatic access and management console access. Enumerated values: • fragment • form_post
signing_key	String	Public key used to sign the ID token of the OpenID Connect identity provider.

Example Request

- Modifying an identity provider that supports programmatic access

```
PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config

{
  "openid_connect_config" : {
    "access_mode" : "program",
    "idp_url" : "https://accounts.example.com",
    "client_id" : "client_id_example",
    "signing_key" : "{\"keys\":[{\"kty\":\"RSA\",\"e\":\"AQAB\",\"use\":\"sig\",\"n\":\"example\",\"kid
\":\"kid_example\",\"alg\":\"RS256\"}]}"
  }
}
```

- Modifying an identity provider that supports programmatic access and management console access

```
PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config

{
  "openid_connect_config" : {
    "access_mode" : "program_console",
    "idp_url" : "https://accounts.example.com",
    "client_id" : "client_id_example",
    "authorization_endpoint" : "https://accounts.example.com/o/oauth2/v2/auth",
    "scope" : "openid",
    "response_type" : "id_token",
    "response_mode" : "form_post",
    "signing_key" : "{\"keys\":[{\"kty\":\"RSA\",\"e\":\"AQAB\",\"use\":\"sig\",\"n\":\"example\",\"kid
\":\"kid_example\",\"alg\":\"RS256\"}]}"
  }
}
```

Example Response

Status code: 200

The request is successful.

```
{
  "openid_connect_config" : {
    "access_mode" : "program_console",
    "idp_url" : "https://accounts.example.com",
    "client_id" : "client_id_example",
    "authorization_endpoint" : "https://accounts.example.com/o/oauth2/v2/auth",
    "scope" : "openid",
    "response_type" : "id_token",
    "response_mode" : "form_post",
```



```
    "signing_key" : "{\"keys\":[{\"kty\":\"RSA\",\"e\":\"AQAB\",\"use\":\"sig\",\"n\":\"example\",\"kid
\":\"kid_example\",\"alg\":\"RS256\"}]}"
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.

Error Codes

For details, see **Error Codes**.

5.13.2.8 Querying an OpenID Connect Identity Provider

Function

This API is provided for the **administrator** to query an OpenID Connect identity provider.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config

Table 5-677 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider ID. Length: 1 to 64 characters

Request Parameters

Table 5-678 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Status code: 200

Table 5-679 Parameters in the response body

Parameter	Type	Description
openid_connect_config	object	OpenID Connect configurations.

Table 5-680 OpenIDConnectConfig

Parameter	Type	Description
access_mode	String	Access type. Options: • **program_console**: programmatic access and management console access. • **program**: programmatic access only.
idp_url	String	URL of the OpenID Connect identity provider. This field corresponds to the **iss** field in the ID token.
client_id	String	ID of a client registered with the OpenID Connect identity provider.
authorization_endpoint	String	Authorization endpoint of the OpenID Connect identity provider. This field is required only if the access type is set to programmatic access and management console access.

Parameter	Type	Description
scope	String	Scopes of authorization requests. This field is required only if the access type is set to programmatic access and management console access. Enumerated values: • openid • email • profile **NOTE** • **openid** must be specified for this field. • A maximum of 10 values can be specified, and they must be separated with spaces. Example: **openid**, **openid email**, **openid profile**, and **openid email profile**.
response_type	String	Response type. This field is required only if the access type is set to programmatic access and management console access. Enumerated value: • id_token
response_mode	String	Response mode. This field is required only if the access type is set to programmatic access and management console access. Enumerated values: • fragment • form_post
signing_key	String	Public key used to sign the ID token of the OpenID Connect identity provider.

Example Request

Request for querying an OpenID Connect identity provider

```
GET https://{address}/v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config
```

Example Response

Status code: 200

The request is successful.

```
{
  "openid_connect_config" : {
    "access_mode" : "program_console",
```



```
    "idp_url" : "https://accounts.example.com",
    "client_id" : "client_id_example",
    "authorization_endpoint" : "https://accounts.example.com/o/oauth2/v2/auth",
    "scope" : "openid",
    "response_type" : "id_token",
    "response_mode" : "form_post",
    "signing_key" : "{\"keys\":[{\"kty\":\"RSA\",\"e\":\"AQAB\",\"use\":\"sig\",\"n\":\"example\",\"kid
\":\"kid_example\",\"alg\":\"RS256\"}]}"
  }
}
```

Status code: 400

Invalid parameters.

```
{
  "error_msg" : "Request body is invalid.",
  "error_code" : "IAM.0011"
}
```

Status code: 401

Authentication failed.

```
{
  "error_msg" : "Request parameter %(key)s is invalid.",
  "error_code" : "IAM.0007"
}
```

Status code: 403

Access denied.

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```

Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal system error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.

Status Code	Description
403	Access denied.
404	The requested resource cannot be found.
500	Internal system error.

Error Codes

For details, see **Error Codes**.

5.13.3 Mappings

5.13.3.1 Listing Mappings

Function

This API is used to list all mappings.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/OS-FEDERATION/mappings

Request Parameters

Table 5-681 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-682 Parameters in the response body

Parameter	Type	Description
links	Links object	Resource link information.
mappings	Array of MappingResult objects	Mapping information.

Table 5-683 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-684 mappings

Parameter	Type	Description
id	String	Mapping ID.
links	Object	Mapping resource link information.
rules	Array of objects	Rule used to map federated users to local users.

Table 5-685 mappings.links

Parameter	Type	Description
self	String	Resource link.

Table 5-686 mappings.rules

Parameter	Type	Description
local	Array of RulesLocal objects	Federated user information on the cloud platform. **user** indicates the name of a federated user on the cloud platform. **group** indicates the group to which a federated user belongs on the cloud platform.

Parameter	Type	Description
remote	Array<Object>	Federated user information in the IdP system. This field is an expression consisting of assertion attributes and operators. The value of this field is determined by the assertion.

Table 5-687 mappings.rules.local

Parameter	Type	Description
user	user object	Name of a federated user on the cloud platform.
group	group object	User group to which a federated user belongs on the cloud platform.
groups	String	User groups to which a federated user belongs on the cloud platform.

Table 5-688 mappings.rules.local.user

Parameter	Type	Description
name	string	Name of a federated user on the cloud platform.

Table 5-689 mappings.rules.local.group

Parameter	Type	Description
name	string	User group to which a federated user belongs on the cloud platform.

Table 5-690 mappings.rules.remote

Parameter	Type	Description
type	String	IdP assertion (SAML) or ID token (OIDC)
any_one_of	Array of strings	The rule is matched only if the specified strings appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. In a **remote** array, **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.

Parameter	Type	Description
not_any_of	Array of strings	The rule is matched only if the specified strings do not appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.

Example Request

Request for querying mappings

```
GET https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings
```

Example Response

Status code: 200

The request is successful.

```
{
    "mappings": [
        {
            "rules": [
                {
                    "local": [
                        {
                            "user": {
                                "name": "LocalUser"
                            }
                        },
                        {
                            "group": {
                                "name": "LocalGroup"
                            }
                        }
                    ],
                    "remote": [
                        {
                            "type": "UserName"
                        },
                        {
                            "type": "orgPersonType",
                            "not_any_of": [
                                "Contractor",
                                "Guest"
                            ]
                        }
                    ]
                }
            ],
            "id": "ACME",
            "links": {
                "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings/ACME"
            }
        }
    ],
    "links": {
        "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings",
        "previous": null,
        "next": null
```



```
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.3.2 Querying Mapping Details

Function

This API is used to query the details of a mapping.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/OS-FEDERATION/mappings/{id}

Table 5-691 URI parameters

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the mapping to be queried.

Request Parameters

Table 5-692 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-693 Parameters in the response body

Parameter	Type	Description
mapping	Object	Mapping information.

Table 5-694 mapping

Parameter	Type	Description
id	String	Mapping ID.
links	Object	Mapping resource link information.
rules	Array of objects	Rule used to map federated users to local users.

Table 5-695 mapping.links

Parameter	Type	Description
self	String	Resource link.

Table 5-696 mappings.rules

Parameter	Type	Description
local	Array of RulesLocal objects	Federated user information on the cloud platform. **user** indicates the name of a federated user on the cloud platform. **group** indicates the group to which a federated user belongs on the cloud platform.
remote	Array<Object>	Federated user information in the IdP system. This field is an expression consisting of assertion attributes and operators. The value of this field is determined by the assertion.

Table 5-697 mappings.rules.local

Parameter	Type	Description
user	user object	Name of a federated user on the cloud platform.
group	group object	User group to which a federated user belongs on the cloud platform.
groups	String	User groups to which a federated user belongs on the cloud platform.

Table 5-698 mappings.rules.local.user

Parameter	Type	Description
name	string	Name of a federated user on the cloud platform.

Table 5-699 mappings.rules.local.group

Parameter	Type	Description
name	string	User group to which a federated user belongs on the cloud platform.

Table 5-700 mapping.rules.remote

Parameter	Type	Description
type	String	IdP assertion (SAML) or ID token (OIDC)

Parameter	Type	Description
any_one_of	Array of strings	The rule is matched only if the specified strings appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. In a **remote** array, **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.
not_any_of	Array of strings	The rule is matched only if the specified strings do not appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.

Example Request

Request for querying mapping details

```
GET https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings/{id}
```

Example Response

Status code: 200

The request is successful.

```
{
   "mapping": {
      "rules": [
         {
            "local": [
               {
                  "user": {
                     "name": "LocalUser"
                  }
               },
               {
                  "group": {
                     "name": "LocalGroup"
                  }
               }
            ],
            "remote": [
               {
                  "type": "UserName"
               },
               {
                  "type": "orgPersonType",
                  "not_any_of": [
                     "Contractor",
                     "Guest"
                  ]
               }
            ]
         }
      ],
      "id": "ACME",
      "links": {
         "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings/ACME"
```



```
    }
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.3.3 Registering a Mapping

Function

This API is provided for the **administrator** to register a mapping.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3/OS-FEDERATION/mappings/{id}

Table 5-701 URI parameters

Parameter	Mandatory	Type	Description
id	Yes	String	Mapping ID.

Request Parameters

Table 5-702 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-703 Parameters in the request body

Parameter	Mandatory	Type	Description
mapping	Yes	Object	Mapping information.

Table 5-704 mapping

Parameter	Mandatory	Type	Description
rules	Yes	Array of objects	Rule used to map federated users to local users.

Table 5-705 mapping.rules

Parameter	Mandatory	Type	Description
local	Yes	Array of RulesLocal objects	Federated user information on the cloud platform. **user** indicates the name of a federated user on the cloud platform. **group** indicates the group to which a federated user belongs on the cloud platform.

Parameter	Mandatory	Type	Description
remote	Yes	Array of objects	Federated user information in the IdP system. If SAML is used, this field is an expression consisting of assertion attributes and operators, and the value of this field is determined by the assertion. If OIDC protocol is used, the value of this field is determined by the ID token.

Table 5-706 mappings.rules.local

Parameter	Mandatory	Type	Description
user	No	user object	Name of a federated user on the cloud platform.
group	No	group object	User group to which a federated user belongs on the cloud platform.
groups	No	String	User groups to which a federated user belongs on the cloud platform.

Table 5-707 mappings.rules.local.user

Parameter	Mandatory	Type	Description
name	Yes	string	Name of a federated user on the cloud platform.

Table 5-708 mappings.rules.local.group

Parameter	Mandatory	Type	Description
name	Yes	string	User group to which a federated user belongs on the cloud platform.

Table 5-709 mapping.rules.remote

Parameter	Mandatory	Type	Description
type	Yes	String	IdP assertion (SAML) or ID token (OIDC)
any_one_of	No	Array of strings	The rule is matched only if the specified strings appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. In a **remote** array, **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.
not_any_of	No	Array of strings	The rule is matched only if the specified strings do not appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.

Response Parameters

Table 5-710 Parameters in the response body

Parameter	Type	Description
mapping	Object	Mapping information.

Table 5-711 mapping

Parameter	Type	Description
id	String	Mapping ID.
links	Object	Mapping resource link information.
rules	Array of objects	Rule used to map federated users to local users.

Table 5-712 mapping.links

Parameter	Type	Description
self	String	Resource link.

Table 5-713 mappings.rules

Parameter	Type	Description
local	Array<Map<String,Object>>	Federated user information on the cloud platform. **user** indicates the name of a federated user, and **group** indicates the group to which the federated user belongs.
remote	Array<Object>	Federated user information in the IdP system. If SAML is used, this field is an expression consisting of assertion attributes and operators, and the value of this field is determined by the assertion. If OIDC protocol is used, the value of this field is determined by the ID token.

Table 5-714 mappings.rules.local

Parameter	Type	Description
user	user object	Name of a federated user on the cloud platform.
group	group object	User group to which a federated user belongs on the cloud platform.
groups	String	User groups to which a federated user belongs on the cloud platform.

Table 5-715 mappings.rules.local.user

Parameter	Type	Description
name	string	Name of a federated user on the cloud platform.

Table 5-716 mappings.rules.local.group

Parameter	Type	Description
name	string	User group to which a federated user belongs on the cloud platform.

Table 5-717 mapping.rules.remote

Parameter	Type	Description
type	String	IdP assertion (SAML) or ID token (OIDC)
any_one_of	Array of strings	The rule is matched only if the specified strings appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. In a **remote** array, **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.
not_any_of	Array of strings	The rule is matched only if the specified strings do not appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.

Example Request

Request for registering a mapping

```
PUT https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings/{id}
{
    "mapping": {
        "rules": [
            {
                "local": [
                    {
                        "user": {
                            "name": "LocalUser"
                        }
                    },
                    {
                        "group": {
                            "name": "LocalGroup"
                        }
                    }
                ],
                "remote": [
                    {
                        "type": "UserName"
                    },
                    {
                        "type": "orgPersonType",
                        "not_any_of": [
                            "Contractor",
                            "Guest"
                        ]
```



```
            }
         ]
      }
   ]
  }
}
```

Example Response

Status code: 201

The mapping is registered successfully.

```
{
   "mapping": {
      "rules": [
         {
            "local": [
               {
                  "user": {
                     "name": "LocalUser"
                  }
               },
               {
                  "group": {
                     "name": "LocalGroup"
                  }
               }
            ],
            "remote": [
               {
                  "type": "UserName"
               },
               {
                  "type": "orgPersonType",
                  "not_any_of": [
                     "Contractor",
                     "Guest"
                  ]
               }
            ]
         }
      ],
      "id": "ACME",
      "links": {
         "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings/ACME"
      }
   }
}
```

Status Codes

Status Code	Description
201	The mapping is registered successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.

Status Code	Description
405	The method specified in the request is not allowed for the requested resource.
409	A resource conflict occurs.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.3.4 Updating a Mapping

Function

This API is provided for the **administrator** to update a mapping.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PATCH /v3/OS-FEDERATION/mappings/{id}

Table 5-718 URI parameters

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the mapping to be updated.

Request Parameters

Table 5-719 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-720 Parameters in the request body

Parameter	Mandatory	Type	Description
mapping	Yes	Object	Mapping information.

Table 5-721 mapping

Parameter	Mandatory	Type	Description
rules	Yes	Array of objects	Rule used to map federated users to local users.

Table 5-722 mapping.rules

Parameter	Mandatory	Type	Description
local	Yes	Array of RulesLocal objects	Federated user information on the cloud platform. **user** indicates the name of a federated user on the cloud platform. **group** indicates the group to which a federated user belongs on the cloud platform.
remote	Yes	Array of objects	Federated user information in the IdP system. If SAML is used, this field is an expression consisting of assertion attributes and operators, and the value of this field is determined by the assertion. If OIDC protocol is used, the value of this field is determined by the ID token.

Table 5-723 mappings.rules.local

Parameter	Mandatory	Type	Description
user	No	user object	Name of a federated user on the cloud platform.
group	No	group object	User group to which a federated user belongs on the cloud platform.
groups	No	String	User groups to which a federated user belongs on the cloud platform.

Table 5-724 mappings.rules.local.user

Parameter	Mandatory	Type	Description
name	Yes	string	Name of a federated user on the cloud platform.

Table 5-725 mappings.rules.local.group

Parameter	Mandatory	Type	Description
name	Yes	string	User group to which a federated user belongs on the cloud platform.

Table 5-726 mapping.rules.remote

Parameter	Mandatory	Type	Description
type	Yes	String	IdP assertion.
any_one_of	No	Array of strings	The rule is matched only if the specified strings appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. In a **remote** array, **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.

Parameter	Mandatory	Type	Description
not_any_of	No	Array of strings	The rule is matched only if the specified strings do not appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.

Response Parameters

Table 5-727 Parameters in the response body

Parameter	Type	Description
mapping	Object	Mapping information.

Table 5-728 mapping

Parameter	Type	Description
id	String	Mapping ID.
links	Object	Mapping resource link information.
rules	Array of objects	Rule used to map federated users to local users.

Table 5-729 mapping.links

Parameter	Type	Description
self	String	Resource link.

Table 5-730 mappings.rules

Parameter	Type	Description
local	Array<Map<String,Object>>	Federated user information on the cloud platform. **user** indicates the name of a federated user, and **group** indicates the group to which the federated user belongs.

Parameter	Type	Description
remote	Array<Object>	Federated user information in the IdP system. If SAML is used, this field is an expression consisting of assertion attributes and operators, and the value of this field is determined by the assertion. If OIDC protocol is used, the value of this field is determined by the ID token.

Table 5-731 mappings.rules.local

Parameter	Type	Description
user	user object	Name of a federated user on the cloud platform.
group	group object	User group to which a federated user belongs on the cloud platform.
groups	String	User groups to which a federated user belongs on the cloud platform.

Table 5-732 mappings.rules.local.user

Parameter	Type	Description
name	string	Name of a federated user on the cloud platform.

Table 5-733 mappings.rules.local.group

Parameter	Type	Description
name	string	User group to which a federated user belongs on the cloud platform.

Table 5-734 mapping.rules.remote

Parameter	Type	Description
type	String	IdP assertion (SAML) or ID token (OIDC)

Parameter	Type	Description
any_one_of	Array of strings	The rule is matched only if the specified strings appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. In a **remote** array, **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.
not_any_of	Array of strings	The rule is matched only if the specified strings do not appear in the attribute type. The condition result is Boolean rather than the argument that is passed as input. **any_one_of** and **not_any_of** are mutually exclusive and cannot be set at the same time.

Example Request

Request for updating a mapping

```
PATCH https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings/{id}
{
   "mapping": {
      "rules": [
         {
            "local": [
               {
                  "user": {
                     "name": "LocalUser"
                  }
               },
               {
                  "group": {
                     "name": "LocalGroup"
                  }
               }
            ],
            "remote": [
               {
                  "type": "UserName"
               },
               {
                  "type": "orgPersonType",
                  "not_any_of": [
                     "Contractor",
                     "Guest"
                  ]
               }
            ]
         }
      ]
   }
}
```

Example Response

Status code: 200

The request is successful.

```
{
   "mapping": {
```

```
    "rules": [
      {
        "local": [
          {
            "user": {
              "name": "LocalUser"
            }
          },
          {
            "group": {
              "name": "LocalGroup"
            }
          }
        ],
        "remote": [
          {
            "type": "UserName"
          },
          {
            "type": "orgPersonType",
            "not_any_of": [
              "Contractor",
              "Guest"
            ]
          }
        ]
      }
    ],
    "id": "ACME",
    "links": {
      "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings/ACME"
    }
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
409	A resource conflict occurs.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.3.5 Deleting a Mapping

Function

This API is provided for the **administrator** to delete a mapping.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3/OS-FEDERATION/mappings/{id}

Table 5-735 URI parameters

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the mapping to be deleted.

Request Parameters

Table 5-736 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for deleting a mapping

```
DELETE https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/mappings/{id}
```

Example Response

None

Status Codes

Status Code	Description
204	The mapping is deleted successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.4 Protocols

5.13.4.1 Listing Protocols

Function

This API is used to list all protocols.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols

Table 5-737 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider ID.

Request Parameters

Table 5-738 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-739 Parameters in the response body

Parameter	Type	Description
links	Object	Resource link information.
protocols	Array of objects	Protocol information.

Table 5-740 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-741 protocols

Parameter	Type	Description
id	String	Protocol ID.
mapping_id	String	Mapping ID.
links	Object	Protocol resource link information.

Table 5-742 protocols.links

Parameter	Type	Description
identity_provider	String	Identity provider resource link.
self	String	Resource link.

Example Request

Request for querying protocols

```
GET https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols
```

Example Response

Status code: 200

The request is successful.

```
{
    "links": {
        "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/protocols",
        "previous": null,
        "next": null
    },
    "protocols": [
        {
            "mapping_id": "ACME",
            "id": "saml",
            "links": {
                "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME/protocols/
saml",
                "identity_provider": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/
ACME"
            }
        }
    ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.4.2 Querying Protocol Details

Function

This API is used to query the details of a protocol.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}

Table 5-743 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider ID.
protocol_id	Yes	String	ID of the protocol to be queried

Request Parameters

Table 5-744 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-745 Parameters in the response body

Parameter	Type	Description
protocol	Object	Protocol information.

Table 5-746 protocol

Parameter	Type	Description
id	String	Protocol ID
mapping_id	String	Mapping ID.
links	Object	Protocol resource link information.

Table 5-747 protocol.links

Parameter	Type	Description
identity_provider	String	Identity provider resource link.
self	String	Resource link.

Example Request

Request for querying protocol details

```
GET https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}
```

Example Response

Status code: 200

The request is successful.

```
{
   "protocol": {
      "mapping_id": "ACME",
      "id": "saml",
      "links": {
         "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME/protocols/
saml",
         "identity_provider": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME"
      }
   }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.4.3 Registering a Protocol

Function

This API is provided for the **administrator** to associate a protocol with an identity provider after **creating the identity provider**.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}

Table 5-748 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider name.
protocol_id	Yes	String	ID of the protocol to be registered The value of this field can be **saml** or **oidc**.

Request Parameters

Table 5-749 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-750 Parameters in the request body

Parameter	Mandatory	Type	Description
protocol	Yes	Object	Protocol information.

Table 5-751 protocol

Parameter	Mandatory	Type	Description
mapping_id	No	String	Mapping ID.

Response Parameters

Table 5-752 Parameters in the response body

Parameter	Type	Description
protocol	Object	Protocol information.

Table 5-753 protocol

Parameter	Type	Description
id	String	Protocol ID The value of this field can be **saml** or **oidc**.
mapping_id	String	Mapping ID.
links	Object	Protocol resource link information.

Table 5-754 protocol.links

Parameter	Type	Description
identity_provider	String	Identity provider resource link.
self	String	Resource link.

Example Request

Request for registering a protocol

```
PUT https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}
{
    "protocol": {
        "mapping_id": "ACME"
    }
}
```

Example Response

Status code: 201

The request is successful.

```
{
    "protocol": {
        "mapping_id": "ACME",
        "id": "saml",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME/protocols/
saml",
            "identity_provider": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME"
        }
```

```
  }
}
```

Status Codes

Status Code	Description
201	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.4.4 Updating a Protocol

Function

This API is provided for the **administrator** to update the protocol associated with a specified identity provider.

The API can be called using both the global endpoint and region-specific endpoints.

URI

PATCH /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}

Table 5-755 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider name.
protocol_id	Yes	String	ID of the protocol to be updated

Request Parameters

Table 5-756 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-757 Parameters in the request body

Parameter	Mandatory	Type	Description
protocol	Yes	Object	Protocol information.

Table 5-758 protocol

Parameter	Mandatory	Type	Description
mapping_id	No	String	Mapping ID. This parameter is required only if the identity provider type is **iam_user_sso**.

Response Parameters

Table 5-759 Parameters in the response body

Parameter	Type	Description
protocol	Object	Protocol information.

Table 5-760 protocol

Parameter	Type	Description
id	String	Protocol ID
mapping_id	String	Mapping ID.
links	Object	Protocol resource link information.

Table 5-761 protocol.links

Parameter	Type	Description
identity_provider	String	Identity provider resource link.
self	String	Resource link.

Example Request

Request for updating a protocol

```
PATCH https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/
{protocol_id}
{
    "protocol": {
        "mapping_id": "ACME"
    }
}
```

Example Response

Status code: 200

The request is successful.

```
{
    "protocol": {
        "mapping_id": "ACME",
        "id": "saml",
        "links": {
            "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME/protocols/
saml",
            "identity_provider": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/ACME"
        }
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.

Status Code	Description
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
409	A resource conflict occurs.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.4.5 Deleting a Protocol

Function

This API is provided for the **administrator** to delete the protocol associated with a specified identity provider.

The API can be called using both the global endpoint and region-specific endpoints.

URI

DELETE /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}

Table 5-762 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider name.
protocol_id	Yes	String	ID of the protocol to be deleted

Request Parameters

Table 5-763 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

None

Example Request

Request for deleting a protocol

```
DELETE https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}
```

Example Response

None

Status Codes

Status Code	Description
204	The protocol is deleted successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.5 Metadata

5.13.5.1 Querying a Metadata File

Function

This API is provided for the **administrator** to query the metadata file imported to IAM for an identity provider.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata

Table 5-764 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider name.
protocol_id	Yes	String	Protocol ID.

Request Parameters

Table 5-765 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Response Parameters

Table 5-766 Parameters in the response body

Parameter	Type	Description
id	String	Metadata file ID.
idp_id	String	Identity provider name.
entity_id	String	Value of **entityID** field in the metadata file.
protocol_id	String	Protocol ID.
domain_id	String	Account ID.
xaccount_type	String	Account source. This parameter is left blank by default.
update_time	String	Time when the metadata file is imported or updated. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
data	String	Content of the metadata file.

Example Request

Request for querying a metadata file

```
GET https://iam.myhuaweicloud.eu/v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata
```

Example Response

Status code: 200

The request is successful.

```
{
    "domain_id": "d78cbac186b744899480f25bd022f468",
    "update_time": "2020-02-12T13:26:25.000000",
    "data": "<md:EntityDescript...",
    "idp_id": "ACME",
    "protocol_id": "saml",
    "id": "11354739a6c940bc899fd9070ed1036d",
    "entity_id": "https://idp.test.com/idp/shibboleth",
    "xaccount_type": ""
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
500	Internal server error.

Error Codes

None

5.13.5.2 Querying the Metadata File of Keystone

Function

This API is used to query the metadata file of Keystone.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3-ext/auth/OS-FEDERATION/SSO/metadata

Request Parameters

Table 5-767 Parameters in the request header

Parameter	Mandatory	Type	Description
unsigned	No	Boolean	Indicates whether to sign metadata according to SAML 2.0. The default value of this parameter is **false**.

Response Parameters

None

Example Request

Request for querying the metadata file of Keystone

```
GET https://iam.myhuaweicloud.eu/v3-ext/auth/OS-FEDERATION/SSO/metadata
```


Example Response

Status code: 200

The request is successful.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor ID="Mc106d5b14b70a4945fa270d8b52d0ed" entityID="https://
iam.myhuaweicloud.eu" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
         <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
         <ds:Reference URI="#Mc106d5b14b70a4945fa270d8b52d0ed">
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
               <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>GmS+Nvta/AvNy4fE7dFID5D+P1U=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>ljRL...</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>
            <ds:X509Certificate>MIIC...</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <md:SPSSODescriptor WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:KeyDescriptor use="signing">
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
               <ds:X509Certificate>MIIC...</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:KeyDescriptor use="encryption">
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
               <ds:X509Certificate>MIIC...</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:NameIDFormat
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">urn:oasis:names:tc:SAML:2.0:nameid-format:transient</
md:NameIDFormat>
      <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://iam.myhuaweicloud.eu/v3-ext/auth/OS-FEDERATION/SSO/SAML2/POST" index="0"
isDefault="true" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"/>
      <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS"
Location="https://iam.myhuaweicloud.eu/v3-ext/auth/OS-FEDERATION/SSO/SAML2/ECP" index="1"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"/>
   </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Status Codes

Status Code	Description
200	The request is successful.
500	Internal server error.

Status Code	Description
503	Service unavailable.

Error Codes

None

5.13.5.3 Importing a Metadata File

Function

This API is provided for the **administrator** to import a metadata file.

This API is used to import a metadata file to IAM to implement federated identity authentication. The metadata file specifies API addresses and certificate information in compliance with the SAML 2.0 standard. To obtain the metadata file of your enterprise IdP, contact the enterprise administrator.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata

Table 5-768 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider name.
protocol_id	Yes	String	Protocol ID.

Request Parameters

Table 5-769 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Access token issued to a user to bear its identity and permissions. For details about the permissions required by the token, see **Actions**.

Table 5-770 Parameters in the request body

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Account ID.
xaccount_type	Yes	String	Account source. This parameter is left blank by default.
metadata	Yes	String	Metadata of the IdP server.

Response Parameters

Table 5-771 Parameters in the response body

Parameter	Type	Description
message	String	Import result.

Example Request

Request for importing a metadata file

```
POST https://iam.myhuaweicloud.eu/v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/
{protocol_id}/metadata
{
    "xaccount_type": "",
    "domain_id": "d78cbac186b744899480f25bd...",
    "metadata": "<md:EntityDescript..."
}
```

Example Response

Status code: 201

The metadata file is imported successfully.

```
{
    "message": "Import metadata successful"
}
```

Status Codes

Status Code	Description
201	The metadata file is imported successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
500	Internal server error.

Error Codes

None

5.13.6 Token

5.13.6.1 Obtaining an Unscoped Token (IdP Initiated)

Function

This API is used to obtain an unscoped token through IdP-initiated federated identity authentication.

Unscoped tokens cannot be used for authentication. A federated user can be authenticated only using a scoped token. For details, see **Obtaining a Scoped Token**.

The API can be called using both the global endpoint and region-specific endpoints.

NOTE

- This API can be called using the CLI. The client can call this API to obtain a SAML response in IdP-initiated authentication mode and obtain an unscoped token through a browser.

URI

POST /v3.0/OS-FEDERATION/tokens

Request Parameters

Table 5-772 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	The client must use a browser to transfer SAML response parameters to the server. Therefore, set this parameter to **application/x-www-form-urlencoded**.
X-Idp-Id	Yes	String	Identity provider ID.

Table 5-773 Parameters in the request formData

Parameter	Mandatory	Type	Description
SAMLResponse	Yes	String	Response body to be returned if IdP authentication is successful.

Perform the following procedure to obtain a SAML response:

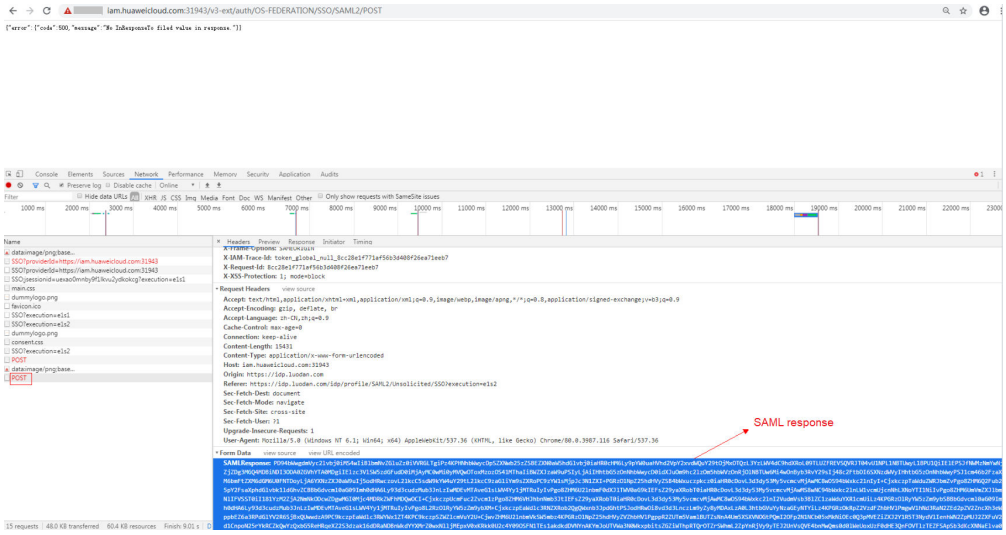
1. Visit **https://*idp.example.org*/idp/profile/SAML2/Unsolicited/SSO?providerId=*iam.example.com*** using a browser.

   idp.example.org: Entity ID in the IdP metadata

   iam.example.com: Entity ID in the SP metadata

2. On the displayed identity provider login page, enter a username and then click **Login** (password-free login is supported). On the new page that is displayed, press **F12** and click **Accept**. Obtain the SAML response from POST as shown in the following figure.

   Figure 5-6 Obtaining a SAML response



Response Parameters

Table 5-774 Parameters in the response header

Parameter	Type	Description
X-Subject-Token	String	Signed unscoped token.

Table 5-775 Parameters in the response body

Parameter	Type	Description
token	Object	Details of the unscoped token.

Table 5-776 token

Parameter	Type	Description
issued_at	String	Time when the token was issued. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
expires_at	String	Time when the token will expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
methods	Array of strings	Method for obtaining the token.
user	Object	Information about the IAM user who requests for the token.

Table 5-777 token.user

Parameter	Type	Description
domain	Object	Information about the account used to create the IAM user.
id	String	User ID.
name	String	Username.

Parameter	Type	Description
OS-FEDERATION	Object	Federated identity authentication information.

Table 5-778 token.user.domain

Parameter	Type	Description
name	String	Account name.
id	String	Account ID.

Table 5-779 token.user.OS-FEDERATION

Parameter	Type	Description
groups	Array of objects	User group information.
identity_provider	Object	Identity provider information.
protocol	Object	Protocol information.

Table 5-780 token.user.OS-FEDERATION.groups

Parameter	Type	Description
id	String	User group ID.
name	String	User group name.

Table 5-781 token.user.OS-FEDERATION.identity_provider

Parameter	Type	Description
id	String	Identity provider ID.

Table 5-782 token.user.OS-FEDERATION.protocol

Parameter	Type	Description
id	String	Protocol ID.

Example Request

Request for obtaining an unscoped token (IdP initiated)

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-FEDERATION/tokens
SAMLResponse=PD94b...
```

Example Response

Status code: 201

The request is successful.

```
Parameters in the response header
X-Subject-Token:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...
Parameters in the response body
{
    "token": {
        "expires_at": "2020-02-13T14:21:34.042000Z",
        "methods": [
            "mapped"
        ],
        "issued_at": "2020-02-12T14:21:34.042000Z",
        "user": {
            "OS-FEDERATION": {
                "identity_provider": {
                    "id": "ACME"
                },
                "protocol": {
                    "id": "saml"
                },
                "groups": [
                    {
                        "id": "06aa22601502cec4a23ac0084a74038f",
                        "name": "admin"
                    }
                ]
            },
            "domain": {
                "name": "IAMDomain",
                "id": "06ba0970a097acc0f36c0086bb6cfe0"
            },
            "name": "FederationUser",
            "id": "LdUTYSC7zmJVIic3yaCbLBXDxPAdDxLg"
        }
    }
}
```

Status Codes

Status Code	Description
201	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
405	The method specified in the request is not allowed for the requested resource.

Status Code	Description
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.6.2 Obtaining a Scoped Token

Function

This API is used to obtain a scoped token through federated identity authentication.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3/auth/tokens

Request Parameters

Table 5-783 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	No	String	Fill **application/json;charset=utf8** in this field.

Table 5-784 Parameters in the request body

Parameter	Mandatory	Type	Description
auth	Yes	Object	Authentication information.

Table 5-785 auth

Parameter	Mandatory	Type	Description
identity	Yes	Object	Authentication parameters.
scope	Yes	Object	Application scope of the token. The value can be **project** or **domain**.

Table 5-786 auth.identity

Parameter	Mandatory	Type	Description
methods	Yes	Array of strings	Authentication method. The value of this field is **token**.
token	Yes	Object	Unscoped token information.

Table 5-787 auth.identity.token

Parameter	Mandatory	Type	Description
id	Yes	String	Unscoped token ID.

Table 5-788 auth.scope

Parameter	Mandatory	Type	Description
domain	No	Object	If this field is set to **domain**, the token can be used to access resources in all projects under the account of a specified ID or name.
project	No	Object	If this field is set to **project**, the token can only be used to access resources in the project of a specified ID or name.

Table 5-789 auth.scope.domain

Parameter	Mandatory	Type	Description
id	No	String	Account ID. Either **id** or **name** must be specified.
name	No	String	Account name. Either **id** or **name** must be specified.

Table 5-790 auth.scope.project

Parameter	Mandatory	Type	Description
domain	No	Object	Account information. This parameter is mandatory if the **name** parameter is set.
id	No	String	Project ID. Either **id** or **name** must be specified.
name	No	String	Project name. Either **id** or **name** must be specified.

Table 5-791 auth.scope.project.domain

Parameter	Mandatory	Type	Description
id	No	string	Account ID. Either **id** or **name** must be specified.
name	No	string	Account name. Either **id** or **name** must be specified.

Response Parameters

Table 5-792 Parameters in the response header

Parameter	Type	Description
X-Subject-Token	String	Signed scoped token.

Table 5-793 Parameters in the response body

Parameter	Type	Description
token	Object	Details of the scoped token.

Table 5-794 token

Parameter	Type	Description
methods	Array of strings	Method for obtaining the token.
expires_at	String	Time when the token will expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
catalog	Array of objects	Catalog information.
domain	Object	Account information of the IAM user who requests for the token. This parameter is returned only when the **scope** parameter in the request body has been set to **domain**.
project	Object	Project information of the IAM user. This parameter is returned only when the **scope** parameter in the request body has been set to **project**.
roles	Array of objects	Permissions information of the token.
user	Object	Information about the IAM user who requests for the token.
issued_at	String	Time when the token was issued. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Table 5-795 token.catalog

Parameter	Type	Description
type	String	Type of the service to which the API belongs.
id	String	Service ID.

Parameter	Type	Description
name	String	Service name.
endpoints	Array of objects	Endpoint information.

Table 5-796 token.catalog.endpoints

Parameter	Type	Description
url	String	Endpoint URL.
region	String	Region to which the endpoint belongs.
region_id	String	Region ID.
interface	String	Visibility of the API. **public** indicates that the API is available for public access.
id	String	Endpoint ID.

Table 5-797 token.domain

Parameter	Type	Description
name	String	Account name.
id	String	Account ID.

Table 5-798 token.project

Parameter	Type	Description
name	String	Project name.
id	String	Project ID.
domain	Object	Account information of the project.

Table 5-799 token.project.domain

Parameter	Type	Description
name	String	Account name.
id	String	Account ID.

Table 5-800 token.roles

Parameter	Type	Description
name	String	Permission name.
id	String	Permission ID. The default value is **0**, which does not correspond to any permission.

Table 5-801 token.user

Parameter	Type	Description
domain	Object	Information about the account used to create the IAM user.
OS-FEDERATION	Object	Federated identity authentication information.
id	String	User ID.
name	String	Username.
password_expires_at	String	Password expiration time. If this parameter is not specified, the password will never expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.

Table 5-802 token.user.domain

Parameter	Type	Description
name	String	Account name.
id	String	Account ID.

Table 5-803 token.user.OS-FEDERATION

Parameter	Type	Description
groups	Array of objects	User group information.
identity_provider	Object	Identity provider information.
protocol	Object	Protocol information.

Table 5-804 token.user.OS-FEDERATION.groups

Parameter	Type	Description
id	String	User group ID.
name	String	User group name.

Table 5-805 token.user.OS-FEDERATION.identity_provider

Parameter	Type	Description
id	String	Identity provider ID.

Table 5-806 token.user.OS-FEDERATION.protocol

Parameter	Type	Description
id	String	Protocol ID.

Example Request

Request for obtaining a scoped token

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens
{
    "auth": {
        "identity": {
            "methods": [
                "token"
            ],
            "token": {
                "id": "MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB..."
            }
        },
        "scope": {
            "domain": {
                "id": "063bb260a480cecc0f36c0086bb6c..."
            }
        }
    }
}
```

Example Response

Status code: 201

The request is successful.

```
Parameters in the response header
X-Subject-Token:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...
Parameters in the response body
{
    "token": {
        "expires_at": "2020-02-13T14:21:34.042000Z",
        "methods": [
```



```
        "token"
    ],
    "catalog": [
        {
            "endpoints": [
                {
                    "id": "d2983f677ce14f1e81cbb6a9345a107a",
                    "interface": "public",
                    "region": "*",
                    "region_id": "*",
                    "url": "https://iam.myhuaweicloud.eu/v3"
                }
            ],
            "id": "fd631b3426cb40f0919091d5861d8fea",
            "name": "keystone",
            "type": "identity"
        }
    ],
    "domain": {
        "id": "06aa2260a480cecc0f36c0086bb6cfe0",
        "name": "IAMDomain"
    },
    "roles": [
        {
            "id": "0",
            "name": "te_admin"
        },
        {
            "id": "0",
            "name": "secu_admin"
        }
    ],
    "issued_at": "2020-02-12T14:21:34.042000Z",
    "user": {
        "OS-FEDERATION": {
            "groups": [
                {
                    "id": "06aa2260bb00cecc3f3ac0084a74038f",
                    "name": "admin"
                }
            ],
            "identity_provider": {
                "id": "ACME"
            },
            "protocol": {
                "id": "saml"
            }
        },
        "domain": {
            "id": "06aa2260a480cecc0f36c0086bb6cfe0",
            "name": "IAMDomain"
        },
        "id": "LdQTDSC7zmJVIic3yaCbLBXDxPAdDxLg",
        "name": "FederationUser",
        "password_expires_at": ""
    }
  }
}
```


Status Codes

Status Code	Description
201	The request is successful.
400	Invalid parameters.

Status Code	Description
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.13.6.3 Obtaining a Token with an OpenID Connect ID Token

Function

This API is used to obtain a federated identity authentication token using an OpenID Connect ID token.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3.0/OS-AUTH/id-token/tokens

Request Parameters

Table 5-807 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Idp-Id	Yes	String	Identity provider ID.

Table 5-808 Parameter in the request body

Parameter	Mandatory	Type	Description
auth	Yes	object	Details about the **auth** request parameter.

Table 5-809 GetIdTokenAuthParams

Parameter	Mandatory	Type	Description
id_token	Yes	object	Details about an ID token.
scope	No	object	Permission scope of the token you want to obtain. An unscoped token will be obtained if this parameter is not specified.

Table 5-810 GetIdTokenIdTokenBody

Parameter	Mandatory	Type	Description
id	Yes	String	ID token, which is constructed by the enterprise IdP to carry the identity information of federated users. For details about how to obtain an ID token, see the enterprise IdP documentation.

Table 5-811 GetIdTokenIdScopeBody

Parameter	Mandatory	Type	Description
domain	No	object	Domain scope details. Specify a domain or a project.
project	No	object	Project scope details. Specify a project or a domain.

Table 5-812 GetIdTokenScopeDomainOrProjectBody

Parameter	Mandatory	Type	Description
id	No	String	Domain ID or project ID. Specify either this parameter or the **name** parameter.

Parameter	Mandatory	Type	Description
name	No	String	Domain name or project name. Specify either this parameter or the **id** parameter.

Response Parameters

Status code: 201

Table 5-813 Parameters in the response header

Parameter	Type	Description
X-Subject-Token	String	Signed token.

Table 5-814 Parameters in the response body

Parameter	Type	Description
token	object	Details about the obtained token.

Table 5-815 ScopedTokenInfo

Parameter	Type	Description
expires_at	String	Time when the token will expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
methods	Array of strings	Method for obtaining the token. For federated users, the default value of this parameter is **mapped**.
issued_at	String	Time when the token was issued. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
user	object	User details.

Parameter	Type	Description
domain	object	Account details.
project	object	Project details.
roles	Array of objects	Role or policy details.
catalog	Array of objects	Catalog details.

Table 5-816 FederationUserBody

Parameter	Type	Description
OS-FEDERATION	object	Federated user details.
domain	object	Account details.
id	String	User ID.
name	String	Username.

Table 5-817 OSFederationInfo

Parameter	Type	Description
identity_provider	object	Identity provider details.
protocol	object	Protocol details.
groups	Array of objects	User group details.

Table 5-818 IdpIdInfo

Parameter	Type	Description
id	String	Identity provider ID.

Table 5-819 ProtocolIdInfo

Parameter	Type	Description
id	String	Protocol ID.

Table 5-820 token.user.OS-FEDERATION.groups

Parameter	Type	Description
id	String	User group ID.
name	String	User group name.

Table 5-821 token.user.domain

Parameter	Type	Description
id	String	Account ID.
name	String	Account name.

Table 5-822 DomainInfo

Parameter	Type	Description
id	String	Account ID.
name	String	Account name.

Table 5-823 ProjectInfo

Parameter	Type	Description
domain	object	Account details.
id	String	Project ID.
name	String	Project name.

Table 5-824 token.project.domain

Parameter	Type	Description
id	String	Account ID.
name	String	Account name.

Table 5-825 roles

Parameter	Type	Description
id	String	Permission ID.

Parameter	Type	Description
name	String	Permission name.

Table 5-826 CatalogInfo

Parameter	Type	Description
id	String	Endpoint ID.
interface	String	Visibility of the API. **public** indicates that the API is available for public access.
region	String	Region to which the endpoint belongs.
region_id	String	Region ID.
url	String	Endpoint URL.

Example Request

- Request for obtaining a scoped token for a specific project
  POST /v3.0/OS-AUTH/id-token/tokens

```
{
  "auth" : {
    "id_token" : {
      "id" : "eyJhbGciOiJSU..."
    },
    "scope" : {
      "project" : {
        "id" : "46419baef4324...",
        "name" : "eu-west-101"
      }
    }
  }
}
```

- Request for obtaining a scoped token for a specific domain
  POST /v3.0/OS-AUTH/id-token/tokens

```
{
  "auth" : {
    "id_token" : {
      "id" : "eyJhbGciOiJSU..."
    },
    "scope" : {
      "domain" : {
        "id" : "063bb260a480...",
        "name" : "IAMDomain"
      }
    }
  }
}
```

- Request for obtaining an unscoped token
  POST /v3.0/OS-AUTH/id-token/tokens


```
{
  "auth" : {
    "id_token" : {
      "id" : "eyJhbGciOiJSU..."
    }
  }
}
```

Example Response

Status code: 201

The token is obtained successfully.

```
{
  "token" : {
    "expires_at" : "2018-03-13T03:00:01.168000Z",
    "methods" : [ "mapped" ],
    "issued_at" : "2018-03-12T03:00:01.168000Z",
    "user" : {
      "OS-FEDERATION" : {
        "identity_provider" : {
          "id" : "idptest"
        },
        "protocol" : {
          "id" : "oidc"
        },
        "groups" : [ {
          "name" : "admin",
          "id" : "45a8c8f..."
        } ]
      },
      "domain" : {
        "id" : "063bb260a480...",
        "name" : "IAMDomain"
      },
      "name" : "FederationUser",
      "id" : "suvmgvUZc4PaCOEc..."
    }
  }
}
```

Status code: 400

Invalid parameters.

```
{
  "error_msg" : "Request body is invalid.",
  "error_code" : "IAM.0011"
}
```

Status code: 401

Authentication failed.

```
{
  "error_msg" : "The request you have made requires authentication.",
  "error_code" : "IAM.0001"
}
```

Status code: 403

Access denied.

```
{
  "error_msg" : "Policy doesn't allow %(actions)s to be performed.",
  "error_code" : "IAM.0003"
}
```


Status code: 404

The requested resource cannot be found.

```
{
  "error_msg" : "Could not find %(target)s: %(target_id)s.",
  "error_code" : "IAM.0004"
}
```

Status code: 500

Internal system error.

```
{
  "error_msg" : "An unexpected error prevented the server from fulfilling your request.",
  "error_code" : "IAM.0006"
}
```

Status Codes

Status Code	Description
201	The token is obtained successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
500	Internal system error.

Error Codes

For details, see **Error Codes**.

5.13.6.4 Obtaining an Unscoped Token with an OpenID Connect ID Token

Function

This API is used to obtain an unscoped token using an OpenID Connect ID token.

The API can be called using both the global endpoint and region-specific endpoints.

URI

POST /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/auth

Table 5-827 URI parameters

Parameter	Mandatory	Type	Description
idp_id	Yes	String	Identity provider name.
protocol_id	Yes	String	Protocol ID.

Request Parameters

Table 5-828 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	ID token of the identity provider. The format is **Bearer** *{ID Token}*.

Response Parameters

Status code: 201

Table 5-829 Parameters in the response header

Parameter	Type	Description
X-Subject-Token	String	Signed token.

Table 5-830 Parameters in the response body

Parameter	Type	Description
token	object	Details about the obtained token.

Table 5-831 UnscopedTokenInfo

Parameter	Type	Description
expires_at	String	Time when the token will expire. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
methods	Array of strings	Token obtaining method. The default value for federated authentication is **mapped**.
issued_at	String	Time when the token was issued. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see **ISO-8601**.
user	object	User details.
roles	Array of objects	Role or policy details.
catalog	Array of objects	Catalog details.

Table 5-832 FederationUserBody

Parameter	Type	Description
OS-FEDERATION	object	Federated user details.
domain	object	Account details.
id	String	User ID.
name	String	Username.

Table 5-833 OSFederationInfo

Parameter	Type	Description
identity_provider	object	Identity provider details.
protocol	object	Protocol details.
groups	Array of objects	User group details.

Table 5-834 IdpIdInfo

Parameter	Type	Description
id	String	Identity provider ID.

Table 5-835 ProtocolIdInfo

Parameter	Type	Description
id	String	Protocol ID.

Table 5-836 token.user.OS-FEDERATION.groups

Parameter	Type	Description
id	String	User group ID.
name	String	User group name.

Table 5-837 DomainInfo

Parameter	Type	Description
id	String	Account ID.
name	String	Account name.

Table 5-838 token.roles

Parameter	Type	Description
id	String	Permission ID.
name	String	Permission name.

Table 5-839 token.catalog

Parameter	Type	Description
id	String	Endpoint ID.
interface	String	Visibility of the API. **public** indicates that the API is available for public access.
region	String	Region to which the endpoint belongs.

Parameter	Type	Description
region_id	String	Region ID.
url	String	Endpoint URL.

Example Request

Request for obtaining an unscoped token with an OpenID Connect ID token

```
POST https://{address}/v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/auth
```

Example Response

Status code: 201

The token is obtained successfully.

```
{
  "token" : {
    "expires_at" : "2018-03-13T03:00:01.168000Z",
    "methods" : [ "mapped" ],
    "issued_at" : "2018-03-12T03:00:01.168000Z",
    "user" : {
      "OS-FEDERATION" : {
        "identity_provider" : {
          "id" : "idptest"
        },
        "protocol" : {
          "id" : "oidc"
        },
        "groups" : [ {
          "name" : "admin",
          "id" : "45a8c8f..."
        } ]
      },
      "domain" : {
        "id" : "063bb260a480...",
        "name" : "IAMDomain"
      },
      "name" : "FederationUser",
      "id" : "suvmgvUZc4PaCOEc..."
    }
  }
}
```

Status code: 400

Invalid parameters.

```
{
  "error" : {
    "code" : 400,
    "message" : "Request parameter 'idp id' is invalid.",
    "title" : "Bad Request"
  }
}
```

Status code: 401

Authentication failed.

```
{
  "error" : {
```



```
    "code" : 401,
    "message" : "The request you have made requires authentication.",
    "title" : "Unauthorized"
  }
}
```

Status code: 403

Access denied.

```
{
  "error" : {
    "code" : 403,
    "message" : "You are not authorized to perform the requested action.",
    "title" : "Forbidden"
  }
}
```

Status code: 404

The server could not find the requested page.

```
{
  "error" : {
    "code" : 404,
    "message" : "Could not find %(target)s: %(target_id)s.",
    "title" : "Not Found"
  }
}
```

Status code: 500

Internal system error.

```
{
  "error" : {
    "code" : 500,
    "message" : "An unexpected error prevented the server from fulfilling your request.",
    "title" : "Internal Server Error"
  }
}
```

Status Codes

Status Code	Description
201	The token is obtained successfully.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The server could not find the requested page.
500	Internal system error.

Error Codes

For details, see **Error Codes**.

5.13.7 Listing Accounts Accessible to Federated Users

Function

This API is used to list the accounts whose resources are accessible to federated users.

The API can be called using both the global endpoint and region-specific endpoints.

NOTE

- The API used to **list the accounts accessible to an IAM user** is recommended because it can return the same response.

URI

GET /v3/OS-FEDERATION/domains

Request Parameters

Table 5-840 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Unscoped token.

Response Parameters

Table 5-841 Parameters in the response body

Parameter	Type	Description
domains	Array of objects	Account information.
links	Object	Resource link information.

Table 5-842 domains

Parameter	Type	Description
enabled	Boolean	Indicates whether an account is enabled. **true** (default value) indicates that the account is enabled. **false** indicates that the account is disabled.
id	String	Account ID.
name	String	Account name.

Parameter	Type	Description
links	Object	Account resource link.
description	String	Description of the account.

Table 5-843 domains.links

Parameter	Type	Description
self	String	Resource link.

Table 5-844 links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for querying accounts accessible to federated users

```
GET https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/domains
```

Example Response

Status code: 200

The request is successful.

```
{
    "domains": [
        {
            "description": "",
            "enabled": true,
            "id": "d78cbac186b744899480f25bd022f468",
            "links": {
                "self": "https://iam.myhuaweicloud.eu/v3/domains/d78cbac186b744899480f25bd022f468"
            },
            "name": "IAMDomain"
        }
    ],
    "links": {
        "self": "https://iam.myhuaweicloud.eu/v3/OS-FEDERATION/domains"
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.

Status Code	Description
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.14 Custom Identity Brokers

5.14.1 Obtaining a Login Token

Function

This API is used to obtain a login token for logging in through a custom identity broker. Login tokens are issued to users to log in through custom identity brokers. Each login token contains identity and session information of a user. To log in to a cloud service console using a custom identity broker URL, call this API to obtain a login token for authentication.

The API can be called using both the global endpoint and region-specific endpoints.

NOTE

By default, a login token is valid for 10 minutes. You can set a validity period from 10 minutes to 12 hours.

URI

POST /v3.0/OS-AUTH/securitytoken/logintokens

Request Parameters

Table 5-845 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

Table 5-846 Parameters in the request body

Parameter	Mandatory	Type	Description
auth	Yes	Object	Authentication information.

Table 5-847 auth

Parameter	Mandatory	Type	Description
securitytoken	Yes	Object	Authentication parameters.

Table 5-848 auth.securitytoken

Parameter	Mandatory	Type	Description
access	Yes	String	AK.
secret	Yes	String	SK.

Parameter	Mandatory	Type	Description
id	Yes	String	Temporary security token. A login token can be obtained using the security token of a custom identity broker user or a common user. For details, see **Obtaining a Temporary Access Key and Security Token Through a Token**. A security token can be obtained using an agency, and the **session_user.name** parameter must be specified in the request body. For details, see **Obtaining a Temporary Access Key and Security Token Through an Agency**.

duration_seconds	No	Integer	Validity period (seconds) of the login token. The value ranges from 10 minutes to 12 hours. The default value is 10 minutes, that is, 600 seconds.
			NOTE
			• If the transferred value is beyond the range (10 minutes to 12 hours), the default value 10 minutes is used.
			• The validity period of the login token is the remaining validity period of the temporary security token or the value of **duration_seconds**, whichever is smaller.
			  • Set a long validity period (15 minutes to 24 hours) for the security token and ensure that the value of **duration_seconds** is less than the remaining validity period of the security token.
			  • If the remaining validity period of the security token is less than 10 minutes, the validity period of the login token is 10 minutes.

Response Parameters

Table 5-849 Parameters in the response header

Parameter	Type	Description
X-Subject-LoginToken	String	Signed login token.

Table 5-850 Parameters in the response body

Parameter	Type	Description
logintoken	Object	Login token information.

Table 5-851 logintoken

Parameter	Type	Description
domain_id	String	Account ID.
expires_at	String	Time when the login token will expire.
method	String	Authentication method. The value is **federation_proxy** for a custom identity broker user and is **token** for a Huawei Cloud user.
user_id	String	User ID.
user_name	String	Username.
session_id	String	Session ID.
session_user_id	String	ID of a custom identity broker user.
session_name	String	Name of a custom identity broker user. **NOTE** This parameter will be returned when you **obtain a temporary access key and security token using an agency** and specify the **session_user.name** parameter in the request body. The value of this parameter is the value of **session_user.name**.
assumed_by	Object	Information about the delegated party. **NOTE** This parameter will be returned when you **obtain a temporary access key and security token using an agency** and specify the **session_user.name** parameter in the request body.

Table 5-852 logintoken.assumed_by

Parameter	Type	Description
user	Object	Information about the delegated party.

Table 5-853 logintoken.assumed_by.user

Parameter	Type	Description
domain	Object	Delegated account information.
name	String	Username of the delegated party.
password_expires_at	String	Expiration time of the password. **NOTE** The value is a UTC time in the YYYY-MM-DDTHH:mm:ss.ssssssZ format, for example, 2023-06-28T08:56:33.710000Z. For details about the date and timestamp formats, see ISO-8601.
id	String	User ID.

Table 5-854 logintoken.assumed_by.user.domain

Parameter	Type	Description
name	String	Name of the account to which the delegated party belongs.
id	String	Account ID.

Example Request

Request for obtaining a login token through a custom identity broker

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-AUTH/securitytoken/logintokens
{
    "auth": {
        "securitytoken": {
            "access": "LUJHNN4WB569PGAP...",
            "secret": "7qtrm2cku0XubixiVkBOcvMfpnu7H2mLN...",
            "id": "gQpjbi1ub3J0a...",
            "duration_seconds":"600"
        }
    }
}
```

Example Response

Status code: 201

The request is successful.

Example 1: Response to the request for obtaining a temporary access key and security token through a token

Example 2: Response to the request for obtaining a temporary access key and security token through an agency (with **session_user.name** in the request body)

- Example 1

  ```
  Parameters in the response header
  X-Subject-LoginToken:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...
  ```

```
Parameters in the response body
{
   "logintoken": {
      "domain_id": "05262121fb00d5c30fbec013bc1...",
      "expires_at": "2020-01-20T08:18:36.447000Z",
      "method": "token",
      "user_id": "0526213b8a80d38a1f31c013ed...",
      "user_name": "IAMUser",
      "session_user_id": "093f75808b8089ba1f6dc000c7cac...",
      "session_id": "40b328b6683a41b9bf8e7185e..."
   }
}
```

- Example 2

```
Parameters in the response header
X-Subject-LoginToken:MIIatAYJKoZIhvcNAQcCoIIapTCCGqECAQExDTALB...
Parameters in the response body
{
   "logintoken": {
      "domain_id": "05262121fb00d5c30fbec01...",
      "expires_at": "2020-01-23T03:27:26.728000Z",
      "method": "federation_proxy",
      "user_id": "07826f367b80d2474ff9c013a...",
      "user_name": "IAMDomainA/IAMAgency",
      "session_id": "0012c8e6adda4ce787e90585d...",
      "session_user_id": "093f75808b8089ba1f6dc000c7cac...",
      "session_name": "SessionUserName",
      "assumed_by": {
         "user": {
            "domain": {
               "name": "IAMDomainB",
               "id": "0659ef9c9c80d4560f14c009ac..."
            },
            "name": "IAMUserB",
            "password_expires_at": "2020-02-16T02:44:57.000000Z",
            "id": "0659ef9d4d00d3b81f26c009fe..."
         }
      }
   }
}
```

Status Codes

Status Code	Description
201	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
500	Internal server error.
503	Service unavailable.

Error Codes

None

5.15 Version Information Management

5.15.1 Querying the Version Information of Keystone APIs

Function

This API is used to query the version information of Keystone APIs.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /

Request Parameters

None

Response Parameters

Table 5-855 Parameters in the response body

Parameter	Type	Description
versions	Object	Keystone API version information.

Table 5-856 versions

Parameter	Type	Description
values	Array of objects	Keystone API version information.

Table 5-857 versions.values

Parameter	Type	Description
status	String	Version status.
updated	String	Time when the API was last updated.
links	Array of objects	Version resource link information.

Parameter	Type	Description
id	String	Version number, for example, **v3.6**.
media-types	Array of objects	Supported message formats.

Table 5-858 versions.values.links

Parameter	Type	Description
rel	String	Link type. • **self**: Versioned link to a resource. • **bookmark**: Permanent link to a resource. • **alternate**: Alternate link to a resource.
href	String	Resource link

Table 5-859 versions.values.media-types

Parameter	Type	Description
type	String	Media type.
base	String	Basic data type.

Example Request

Request for querying the version information of Keystone APIs

```
GET https://iam.myhuaweicloud.eu/
```

Example Response

Status code: 300

The request is successful. (Multiple choices)

```
{
   "versions": {
      "values": [
         {
            "media-types": [
               {
                  "type": "application/vnd.openstack.identity-v3+json",
                  "base": "application/json"
               }
            ],
            "links": [
               {
                  "rel": "self",
                  "href": "https://iam.myhuaweicloud.eu/v3/"
               }
```

```
            ],
            "id": "v3.6",
            "updated": "2016-04-04T00:00:00Z",
            "status": "stable"
        }
    ]
  }
}
```

Status Codes

Status Code	Description
300	The request is successful. (Multiple choices)
400	Invalid parameters.
404	The requested resource cannot be found.
503	Service unavailable.

Error Codes

None

5.15.2 Querying Information About Keystone API 3.0

Function

This API is used to obtain the information about Keystone API 3.0.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3

Request Parameters

None

Response Parameters

Table 5-860 Parameters in the response body

Parameter	Type	Description
version	Object	Information about Keystone API 3.0.

Table 5-861 version

Parameter	Type	Description
status	String	Version status.
updated	String	Time when the API was last updated.
links	Array of objects	Version resource link information.
id	String	Version number, for example, **v3.6**.
media-types	Array of objects	Supported message formats.

Table 5-862 version.links

Parameter	Type	Description
rel	String	Link type. • **self**: Versioned link to a resource. • **bookmark**: Permanent link to a resource. • **alternate**: Alternate link to a resource.
href	String	Resource link.

Table 5-863 version.media-types

Parameter	Type	Description
type	String	Media type.
base	String	Basic data type.

Example Request

Request for querying information about Keystone API 3.0

```
GET https://iam.myhuaweicloud.eu/v3
```

Example Response

Status code: 200

The request is successful.

```
{
    "version": {
        "media-types": [
            {
                "type": "application/vnd.openstack.identity-v3+json",
```

```
            "base": "application/json"
        }
    ],
    "links": [
        {
            "rel": "self",
            "href": "https://iam.myhuaweicloud.eu/v3/"
        }
    ],
    "id": "v3.6",
    "updated": "2016-04-04T00:00:00Z",
    "status": "stable"
  }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
404	The requested resource cannot be found.
503	Service unavailable.

Error Codes

None

5.16 Services and Endpoints

5.16.1 Listing Services

Function

This API is used to list all services.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/services

Table 5-864 Query parameters

Parameter	Mandatory	Type	Description
type	No	String	Service type.

Request Parameters

Table 5-865 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token (no special permission requirements).

Response Parameters

Table 5-866 Parameters in the response body

Parameter	Type	Description
links	Object	Service resource link information.
services	Array of objects	Service information.

Table 5-867 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Table 5-868 services

Parameter	Type	Description
name	String	Service name.

Parameter	Type	Description
description	String	Description of the service.
links	Object	Service resource link.
id	String	Service ID.
type	String	Service type.
enabled	Boolean	Enabling status of the service.

Table 5-869 services.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying a list of services

```
GET https://iam.myhuaweicloud.eu/v3/services
```

Example Response

Status code: 200

The request is successful.

```
{
    "links": {
        "next": null,
        "previous": null,
        "self": "https://iam.myhuaweicloud.eu/v3/services"
    },
    "services": [
        {
            "name": "keystone",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://iam.myhuaweicloud.eu/v3/services/1842ae22353d45a39a1eb89c22f0fe50"
            },
            "id": "1842ae22353d45a39a1eb89c22f0fe50",
            "type": "identity",
            "enabled": true
        },
        {
            "name": "iam",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://iam.myhuaweicloud.eu/v3/services/6cf6e23e00dd49beb13313b024aec598"
            },
```

```
        "id": "6cf6e23e00dd49beb13313b024aec598",
        "type": "identity",
        "enabled": true
      }
   ]
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
501	The API is not available.
503	Service unavailable.

Error Codes

None

5.16.2 Querying Service Details

Function

This API is used to query the details of a service.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/services/{service_id}

Table 5-870 URI parameters

Parameter	Mandatory	Type	Description
service_id	Yes	String	ID of the service to be queried.

Request Parameters

Table 5-871 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token (no special permission requirements).

Response Parameters

Table 5-872 Parameters in the response body

Parameter	Type	Description
service	Object	Service information.

Table 5-873 service

Parameter	Type	Description
name	String	Service name.
description	String	Description of the service.
links	Object	Service resource link.
id	String	Service ID.
type	String	Service type.
enabled	Boolean	Enabling status of the service.

Table 5-874 service.links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying service details

```
GET https://iam.myhuaweicloud.eu/v3/services/{service_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "service": {
        "name": "iam",
        "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/services/6cf6e23e00dd49beb13313b024aec598"
        },
        "id": "6cf6e23e00dd49beb13313b024aec598",
        "type": "identity",
        "enabled": true
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
501	The API is not available.
503	Service unavailable.

Error Codes

None

5.16.3 Querying the Service Catalog

Function

This API is used to query the service catalog corresponding to **X-Auth-Token** contained in the request.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/auth/catalog

Request Parameters

Table 5-875 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token (No special permissions are required, but the **scope** of the token must be **project**.)

Response Parameters

Table 5-876 Parameters in the response body

Parameter	Type	Description
catalog	Array of objects	Service catalog information.
links	Object	Resource link information.

Table 5-877 catalog

Parameter	Type	Description
endpoints	Array of objects	Endpoint information.
id	String	Service ID.
name	String	Service name.
type	String	Service type.

Table 5-878 catalog.endpoints

Parameter	Type	Description
id	String	Endpoint ID.
interface	String	Plane to which the endpoint belongs. The value is **public**.
region	String	Region to which the endpoint belongs.
region_id	String	ID of the region to which the endpoint belongs.
url	String	Endpoint URL.

Table 5-879 links

Parameter	Type	Description
self	String	Resource link.

Example Request

Request for querying a service catalog

```
GET https://iam.myhuaweicloud.eu/v3/auth/catalog
```

Example Response

Status code: 200

The request is successful.

```
{
  "catalog": [
    {
      "endpoints": [
        {
          "id": "33e1cbdd86d34e89a63cf8ad16a5f49f",
          "interface": "public",
          "region": "*",
          "region_id": "*",
          "url": "https://iam.myhuaweicloud.eu/v3.0"
        }
      ],
      "id": "100a6a3477f1495286579b819d399e36",
      "name": "iam",
      "type": "iam"
    },
    {
      "endpoints": [
        {
          "id": "6c91faa9890f40b397542561e3d87444",
          "interface": "public",
          "region": "*",
          "region_id": "*",
          "url": "https://cbc.sample.domain.com/v1.0"
        }
```



```
            ],
            "id": "ad7396ee0eea4281a180c4230641b72f",
            "name": "bss-intlv1",
            "type": "bss-intlv1"
        }
    ],
    "links": {
        "self": "https://iam.myhuaweicloud.eu/v3/auth/catalog"
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
501	The API is not available.
503	Service unavailable.

Error Codes

None

5.16.4 Listing Endpoints

Function

This API is used to list all endpoints. An endpoint provides an entry to a specific service.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/endpoints

Table 5-880 Query parameters

Parameter	Mandatory	Type	Description
interface	No	String	Plane to which the endpoint belongs.
service_id	No	String	Service ID.

Request Parameters

Table 5-881 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token (no special permission requirements).

Response Parameters

Table 5-882 Parameters in the response body

Parameter	Type	Description
endpoints	Array of objects	Resource link.
links	Object	Endpoint information.

Table 5-883 endpoints

Parameter	Type	Description
service_id	String	ID of the service to which the endpoint belongs.
region_id	String	ID of the region to which the endpoint belongs.
links	Object	Endpoint resource link information.
id	String	Endpoint ID.
interface	String	Plane to which the endpoint belongs.
region	String	Region to which the endpoint belongs.

Parameter	Type	Description
url	String	Endpoint URL.
enabled	Boolean	Enabling status of the endpoint.

Table 5-884 endpoints.links

Parameter	Type	Description
self	String	Resource link.
next	String	Next resource link.
previous	String	Previous resource link.

Table 5-885 links

Parameter	Type	Description
self	String	Resource link.
previous	String	Previous resource link.
next	String	Next resource link.

Example Request

Request for querying endpoints

```
GET https://iam.myhuaweicloud.eu/v3/endpoints
```

Example Response

Status code: 200

The request is successful.

```
{
  "endpoints": [
    {
      "service_id": "3e93d3eb20b34bfbbdcc81a79c1c3045",
      "region_id": "eu-west-101",
      "links": {
        "next": null,
        "previous": null,
        "self": "https://iam.myhuaweicloud.eu/v3/endpoints/0046cca357c94165b7a10ec2c01bdf60"
      },
      "id": "0046cca357c94165b7a10ec2c01bdf60",
      "interface": "public",
      "region": "eu-west-101",
      "url": "https://ims.sample.domain.com",
      "enabled": true
    },
    {
```



```
            "service_id": "5186586acd38461d84b3dbf9f02e33ae",
            "region_id": "eu-west-101",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://iam.myhuaweicloud.eu/v3/endpoints/00d546d4823e452491407284ab26612c"
            },
            "id": "00d546d4823e452491407284ab26612c",
            "interface": "public",
            "region": "eu-west-101",
            "url": "https://ges.sample.domain.com/v1.0/$(tenant_id)s",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://iam.myhuaweicloud.eu/v3/endpoints"
    }
}
```


Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
501	The API is not available.
503	Service unavailable.

Error Codes

None

5.16.5 Querying Endpoint Details

Function

This API is used to query the details of an endpoint. An endpoint provides an entry to a specific service.

The API can be called using both the global endpoint and region-specific endpoints.

URI

GET /v3/endpoints/{endpoint_id}

Table 5-886 URI parameters

Parameter	Mandatory	Type	Description
endpoint_id	Yes	String	ID of the endpoint to be queried.

Request Parameters

Table 5-887 Parameters in the request header

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.
X-Auth-Token	Yes	String	IAM user token (no special permission requirements).

Response Parameters

Table 5-888 Parameters in the response body

Parameter	Type	Description
endpoint	Object	Endpoint information.

Table 5-889 endpoint

Parameter	Type	Description
service_id	String	ID of the service to which the endpoint belongs.
region_id	String	ID of the region to which the endpoint belongs.
links	Object	Endpoint resource link information.
id	String	Endpoint ID.
interface	String	Plane to which the endpoint belongs.
region	String	Region to which the endpoint belongs.

Parameter	Type	Description
url	String	Endpoint URL.
enabled	Boolean	Enabling status of the endpoint.

Table 5-890 endpoint.links

Parameter	Type	Description
self	String	Resource link.
next	String	Next resource link.
previous	String	Previous resource link.

Example Request

Request for querying endpoint details

```
GET https://iam.myhuaweicloud.eu/v3/endpoints/{endpoint_id}
```

Example Response

Status code: 200

The request is successful.

```
{
    "endpoint": {
        "service_id": "3e93d3eb20b34bfbbdcc81a79c1c3045",
        "region_id": "eu-west-101",
        "links": {
            "next": null,
            "previous": null,
            "self": "https://iam.myhuaweicloud.eu/v3/endpoints/0046cca357c94165b7a10ec2c01bdf60"
        },
        "id": "0046cca357c94165b7a10ec2c01bdf60",
        "interface": "public",
        "region": "eu-west-101",
        "url": "https://ims.sample.domain.com",
        "enabled": true
    }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	Invalid parameters.
401	Authentication failed.

Status Code	Description
403	Access denied.
404	The requested resource cannot be found.
405	The method specified in the request is not allowed for the requested resource.
413	The request entity is too large.
501	The API is not available.
503	Service unavailable.

Error Codes

None

6 Out-of-Date APIs

6.1 Querying User Groups Associated with an Enterprise Project

Function Description

This API is used to query the user groups associated with the enterprise project of a specified ID.

NOTE

This API will be deprecated soon. Please use the API described in **Querying User Groups Associated with an Enterprise Project** instead.

URI

- URI format

  GET /v3.0/OS-PAP/enterprise-projects/{enterprise_project_id}/groups

- URI parameter description

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	ID of the enterprise project for querying associated user groups.

Request

- Request header parameter description

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **Security Administrator** permissions.
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

- Sample request

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https://iam.myhuaweicloud.eu/v3.0/OS-PAP/enterprise-projects/535fb147-6148-4c71-a679-b79a2cb0ee5d/groups
```

Response

- Response body parameter description

Parameter	Mandatory	Type	Description
groups	Yes	Array	Details about the user groups associated with the specified enterprise project.

- User groups format

Parameter	Mandatory	Type	Description
group_id	Yes	String	ID of a user group.
group_name	Yes	String	Name of the user group.
group_desc	Yes	String	Description of the user group.
user_num	Yes	Int	Number of users contained in the user group.
policy_num	Yes	Int	Number of policies that have been configured for the user group.
created_at	Yes	Int	Time when the user group was created. The value is a Unix timestamp in millisecond.

- Example response: Querying an enterprise project with associated user groups

```
{
    "groups": [
        {
            "group_id": "758b99fa1fa24ec4a297d44e092bd...",
            "group_name": "Test",
            "group_desc": "Test",
            "user_num": 4,
```



```
            "policy_num": 1,
            "created_at": 1549088526...
        }
    ]
}
```

- If an enterprise project without any associated user groups is queried, the response body is empty.

```
{
  "groups": []
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	The server failed to process the request.
401	You must enter a username and password to access the requested page.
403	Access denied.
404	The server could not find the requested page.

6.2 Querying the Permissions of a User Group Associated with an Enterprise Project

Function

This API is used to query the permissions of a user group associated with the enterprise project of a specified ID.

This API can be invoked using the global domain name iam.myhuaweicloud.eu.

NOTE

This API will be deprecated soon. Please use the API described in **Querying the Permissions of a User Group Associated with an Enterprise Project** instead.

URI

- URI format

  GET /v3.0/OS-PAP/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles

- URI parameter description

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	ID of the enterprise project for querying the permissions of an associated user group.
group_id	Yes	String	ID of a user group associated with the enterprise project.

Request

- Request header parameter description

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **Security Administrator** permissions.
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

- Sample request

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X GET https://iam.myhuaweicloud.eu/v3.0/OS-PAP/enterprise-projects/535fb147-6148-4c71-a679-b79a2cb0e.../groups/10d8104f395d43468094753f28692.../roles
```

Response

- Response body parameter description

Parameter	Mandatory	Type	Description
roles	Yes	JSONArray	Permission information.

- Description for the role format

Parameter	Mandatory	Type	Description
display_name	Yes	String	Name of a permission displayed on the console.
description	Yes	String	Description of the permission.
description_cn	Yes	String	Description of the permission.

Parameter	Mandatory	Type	Description
domain_id	Yes	String	• If a custom policy has been bound to the user group, the value of this parameter is the account ID of the user that creates the custom policy. • If a default policy has been bound to the user group, the value of this parameter is null.
flag	No	String	A tag for indicating an internal fine-grained role.
catalog	Yes	String	Directory to which the permission belongs. • If a custom policy has been bound to the user group, the value of this parameter is **CUSTOMED**. • If a default policy has been bound to the user group, the value of this parameter is the corresponding service name, for example, **ECS**.
policy	Yes	Dict	Details about the permission. For more information, see **Description for the policy format**.
id	Yes	String	Permission ID.
type	Yes	String	Display position of the permission. • **AX**: Displayed in the Global project. • **XA**: Displayed in projects other than the Global project. **NOTE** The value of this parameter can only be **AX** or **XA**, and cannot be **AA** or **XX**.
name	Yes	String	Name of the permission used in the system.

- Description for the policy format

Parameter	Mandatory	Type	Description
Version	Yes	String	Policy version.
Statement	Yes	JSONArray	Statement for using the policy to grant permissions. A policy consists of a maximum of eight statements. A **Statement** field contains the **Effect** and **Action** elements.

- Description for the statement format

Parameter	Mandatory	Type	Description
Effect	Yes	String	The value can be **Allow** or **Deny**. If both Allow and Deny statements are found in a policy, the authentication starts from the Deny statements.
Action	Yes	StringArray	Permission set, which specifies the operation permissions on resources. The number of permission sets cannot exceed 100. Format: The value format is *Service name*:*Resource type*:*Action*, for example, **vpc:ports:create**. *Service name*: indicates the product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed. *Resource type* and *Action*: The values are case-insensitive, and the wildcard (*) is allowed. A wildcard (*) can represent all or part of the information about resource types and actions for the specific service.

- Example successful response

```
{
  "roles": [
    {
      "display_name": "Customed ECS Viewer",
      "description": "The read-only permissions to all ECS resources, which can be used for statistics and survey.",
      "domain_id": "9698542758bc422088c0c3eabf...",
      "catalog": "CUSTOMED",
```



```
    "policy": {
      "Version": "1.1",
      "Statement": [
        {
          "Action": [
            "ecs:*:get*",
            "ecs:*:list*",
            "ecs:blockDevice:use",
            "ecs:serverGroups:manage",
            "ecs:serverVolumes:use",
            "evs:*:get*",
            "evs:*:list*",
            "vpc:*:get*",
            "vpc:*:list*",
            "ims:*:get*",
            "ims:*:list*"
          ],
          "Effect": "Allow"
        }
      ]
    },
    "id": "24e7a89bffe443979760c4e9715c1...",
    "type": "XA",
    "name": "custom_9698542758bc422088c0c3eabfc30d1..."
  }
 ]
}
```

- Error response body parameter description

Parameter	Mandatory	Type	Description
error	Yes	Dict	Response error
message	Yes	String	Error details
code	Yes	Int	Status code
title	Yes	String	Error type

- Example failed response

```
{
 "error": {
  "message": "Authentication failed",
  "code": 401,
  "title": "Unauthorized"
 }
}
```

Status Codes

Status Code	Description
200	The request is successful.
400	The server failed to process the request.
401	You must enter a username and password to access the requested page.

Status Code	Description
403	Access denied.
500	Failed to complete the request because of an internal service error.

6.3 Granting Permissions to a User Group Associated with an Enterprise Project

Function Description

This API is used to grant permissions to a user group associated with the enterprise project of a specified ID.

This API can be invoked using the global domain name iam.myhuaweicloud.eu.

NOTE

This API will be deprecated soon. Please use the API described in **Granting Permissions to a User Group Associated with an Enterprise Project** instead.

URI

- URI format

  PUT /v3.0/OS-PAP/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}

- URI parameter description

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	ID of an enterprise project.
group_id	Yes	String	ID of a user group to be granted permissions.
role_id	Yes	String	Permission ID. Only fine-grained policies (including default and custom policies) of version 1.1 can be granted to a user group.

Request

- Request header parameter description

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **Security Administrator** permissions.
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

- Sample request

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X PUT https://iam.myhuaweicloud.eu/v3.0/OS-PAP/enterprise-projects/535fb147-6148-4c71-a679-b79a2cb0e.../groups/10d8104f395d43468094753f28692.../roles/013ad036ee4c4d108327f02cbb479...
```

Response

No response body.

Status Codes

Status Code	Description
204	The request is successful.
400	The server failed to process the request.
401	You must enter a username and password to access the requested page.
403	Access denied.
404	The server could not find the requested page.
500	Internal server error.

6.4 Removing the Permissions of a User Group Associated with an Enterprise Project

Function Description

This API is used to remove the permissions of a user group associated with an enterprise project.

This API can be invoked using the global domain name iam.myhuaweicloud.eu.

NOTE

This API will be deprecated soon. Please use the API described in **Removing Permissions of a User Group Associated with an Enterprise Project** instead.

URI

- URI format

  DELETE /v3.0/OS-PAP/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}

- URI parameter description

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	ID of an enterprise project.
group_id	Yes	String	ID of a user group.
role_id	Yes	String	ID of a role (policy) associated with the user group.

Request

- Request header parameter description

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Authenticated token with **Security Administrator** permissions.
Content-Type	Yes	String	Fill **application/json;charset=utf8** in this field.

- Sample request

```
curl -i -k -H "X-Auth-Token:$token" -H 'Content-Type:application/json;charset=utf8' -X DELETE https://iam.myhuaweicloud.eu/v3.0/OS-PAP/enterprise-projects/535fb147-6148-4c71-a679-b79a2cb0e.../groups/10d8104f395d43468094753f28692.../roles/013ad036ee4c4d108327f02cbb479...
```

Response

No response body.

Status Codes

Status Code	Description
204	The request is successful.
400	The server failed to process the request.

Status Code	Description
401	You must enter a username and password to access the requested page.
403	Access denied.
404	The server could not find the requested page.
500	Internal server error.

7 Permissions and Actions

7.1 Permissions and Supported Actions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using **roles** and **policies**. Roles are a type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

NOTE

Policy-based authorization is useful if you want to allow or deny the access to an API.

An account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions allowing the actions can call the API successfully. For example, if an IAM user wants to query ECSs using an API, the user must have been granted permissions that allow the **ecs:servers:list** action.

Supported Actions

IAM provides system-defined policies that can be directly used. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: Statements in a policy that allow or deny certain operations.
- APIs: REST APIs that can be called by a user who has been granted specific permissions.

- Actions: Specific operations that are allowed or denied in **custom policies**.
- IAM or enterprise projects: Type of projects for which an action will take effect. Policies that contain actions for both IAM and enterprise projects can be used and take effect for both IAM and Enterprise Management. Policies that only contain actions for IAM projects can be used and only take effect for IAM. For details about the differences between IAM and enterprise projects, see **What Are the Differences Between IAM Projects and Enterprise Projects?**

NOTE

- The check mark (√) and cross symbol (x) indicate that an action takes effect or does not take effect for the corresponding type of projects. A hyphen (-) indicates that an action is irrelevant to the corresponding type of projects.
- IAM is a global service which does not involve project-based authorization.
- Some permissions support only actions and do not support APIs, such as **permissions for virtual MFA device management**.

7.2 Actions

Token Management

Permission	API	Action	IAM Project	Enterprise Project
Obtaining an Agency Token	**POST /v3/auth/tokens**	iam:tokens:assume	-	-

Access Key Management

Permission	API	Action	IAM Project	Enterprise Project
Listing Permanent Access Keys	**GET /v3.0/OS-CREDENTIAL/credentials**	iam:credentials:listCredentials	-	-
Querying a Permanent Access Key	**GET /v3.0/OS-CREDENTIAL/credentials/{access_key}**	iam:credentials:getCredential	-	-
Creating a Permanent Access Key	**POST /v3.0/OS-CREDENTIAL/credentials**	iam:credentials:createCredential	-	-

Permission	API	Action	IAM Project	Enterprise Project
Modifying a Permanent Access Key	**PUT /v3.0/OS-CREDENTIAL/credentials/{access_key}**	iam:credentials:updateCredential	-	-
Deleting a Permanent Access Key	**DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key}**	iam:credentials:deleteCredential	-	-

Virtual MFA Device Management

Permission	API	Action	IAM Project	Enterprise Project
Binding a Virtual MFA Device	**PUT /v3.0/OS-MFA/mfa-devices/bind**	iam:mfa:bindMFADevice	-	-
Unbinding a Virtual MFA Device	**PUT /v3.0/OS-MFA/mfa-devices/unbind**	iam:mfa:unbindMFADevice	-	-
Generating a Secret Key for Binding a Virtual MFA Device	**POST /v3.0/OS-MFA/virtual-mfa-devices**	iam:mfa:createVirtualMFADevice	-	-
Deleting a Virtual MFA Device	**DELETE /v3.0/OS-MFA/virtual-mfa-devices**	iam:mfa:deleteVirtualMFADevice	-	-

Project Management

Permission	API	Action	IAM Project	Enterprise Project
Listing Projects	**GET /v3/projects**	iam:projects:listProjects	-	-
Creating a Project	**POST /v3/projects**	iam:projects:createProject	-	-

Permission	API	Action	IAM Project	Enterprise Project
Modifying Project Information	**PATCH /v3/projects/{project_id}**	iam:projects:updateProject	-	-
Changing Project Status	**PUT /v3-ext/projects/{project_id}**	iam:projects:updateProject	-	-
Listing the Projects Accessible to a User	**GET /v3/users/{user_id}/projects**	iam:projects:listProjectsForUser	-	-
Deleting a Project	×	iam:projects:deleteProject	-	-
Querying the Quotas of a Project	**GET /v3.0/OS-QUOTA/projects/{project_id}**	iam:quotas:listQuotasForProject	-	-

Account Management

Permission	API	Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Querying the Quotas of an Account	**GET /v3.0/OS-QUOTA/domains/{domain_id}**	iam:quotas:listQuotas	-	-

IAM User Management

Permission	API	Action	IAM Project	Enterprise Project
Listing IAM Users	**GET /v3/users**	iam:users:listUsers	-	-
Creating an IAM User	**POST /v3/users**	iam:users:createUser	-	-
Modifying User Information	**PATCH /v3/users/{user_id}**	iam:users:updateUser	-	-

Permission	API	Action	IAM Project	Enterprise Project
Deleting an IAM User	**DELETE /v3/users/{user_id}**	iam:users:deleteUser	-	-
Creating an IAM User (Recommended)	**POST /v3.0/OS-USER/users**	iam:users:createUser	-	-
Querying IAM User Details (Including Email Address and Mobile Number)	**GET /v3.0/OS-USER/users/{user_id}**	iam:users:getUser	-	-
Querying IAM User Details	**GET /v3/users/{user_id}**	iam:users:getUser	-	-
Resetting an IAM User's Password	×	iam:users:resetUserPassword	-	-
Configuring Login Protection	×	iam:users:setUserLoginProtect	-	-
Listing Users Who Have Access to a Specified Project	×	iam:users:listUsersForProject	-	-
Querying MFA Device Information of IAM Users	**GET /v3.0/OS-MFA/virtual-mfa-devices**	iam:mfa:listVirtualMFADevices	-	-
Querying the MFA Device Information of an IAM User	**GET /v3.0/OS-MFA/users/{user_id}/virtual-mfa-device**	iam:mfa:getVirtualMFADevice	-	-
Querying Login Protection Configurations of IAM Users	**GET /v3.0/OS-USER/login-protects**	iam:users:listUserLoginProtects	-	-

Permission	API	Action	IAM Project	Enterprise Project
Querying the Login Protection Configuration of an IAM User	**GET /v3.0/OS-USER/users/{user_id}/login-protect**	iam:users:getUserLoginProtect	-	-

User Group Management

Permission	API	Action	IAM Project	Enterprise Project
Querying the User Groups to Which an IAM User Belongs	**GET /v3/users/{user_id}/groups**	iam:groups:listGroupsForUser	-	-
Querying the IAM Users in a Group	**GET /v3/groups/{group_id}/users**	iam:users:listUsersForGroup	-	-
Listing User Groups	**GET /v3/groups**	iam:groups:listGroups	-	-
Querying User Group Details	**GET /v3/groups/{group_id}**	iam:groups:getGroup	-	-
Creating a User Group	**POST /v3/groups**	iam:groups:createGroup	-	-
Updating User Group Information	**PATCH /v3/groups/{group_id}**	iam:groups:updateGroup	-	-

Permission	API	Action	IAM Project	Enterprise Project
Deleting a User Group	**DELETE /v3/groups/{group_id}**	iam:groups:deleteGroup iam:permissions:removeUserFromGroup iam:permissions:revokeRoleFromGroup iam:permissions:revokeRoleFromGroupOnProject iam:permissions:revokeRoleFromGroupOnDomain	-	-
Checking Whether an IAM User Belongs to a User Group	**HEAD /v3/groups/{group_id}/users/{user_id}**	iam:permissions:checkUserInGroup	-	-
Adding an IAM User to a User Group	**PUT /v3/groups/{group_id}/users/{user_id}**	iam:permissions:addUserToGroup	-	-
Removing an IAM User from a User Group	**DELETE /v3/groups/{group_id}/users/{user_id}**	iam:permissions:removeUserFromGroup	-	-

Permissions Management

Permission	API	Action	IAM Project	Enterprise Project
Listing Permissions	**GET /v3/roles**	iam:roles:listRoles	-	-
Querying Permission Details	**GET /v3/roles/{role_id}**	iam:roles:getRole	-	-
Querying Permissions Assignment Records	**GET /v3.0/OS-PERMISSION/role-assignments**	iam:permissions:listRoleAssignments	√	√

Permission	API	Action	IAM Project	Enterprise Project
Querying Permissions of a User Group for the Global Service Project	**GET /v3/domains/{domain_id}/groups/{group_id}/roles**	iam:permissions:listRolesForGroupOnDomain	-	-
Querying Permissions of a User Group for a Region-specific Project	**GET /v3/projects/{project_id}/groups/{group_id}/roles**	iam:permissions:listRolesForGroupOnProject	-	-
Granting Permissions to a User Group for the Global Service Project	**PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}**	iam:permissions:grantRoleToGroupOnDomain	-	-
Granting Permissions to a User Group for a Region-specific Project	**PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}**	iam:permissions:grantRoleToGroupOnProject	-	-
Removing Permissions of a User Group for a Region-specific Project	**DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}**	iam:permissions:revokeRoleFromGroupOnProject	-	-
Removing Permissions of a User Group for the Global Service Project	**DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}**	iam:permissions:revokeRoleFromGroupOnDomain	-	-
Checking Whether a User Group Has Specified Permissions for the Global Service Project	**HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}**	iam:permissions:checkRoleForGroupOnDomain	-	-
Checking Whether a User Group Has Specified Permissions for a Region-specific Project	**HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}**	iam:permissions:checkRoleForGroupOnProject	-	-

Permission	API	Action	IAM Project	Enterprise Project
Granting Specified Permissions to a User Group for All Projects	**PUT /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects**	iam:permissions:grantRoleToGroup	-	-
Querying the Permissions Granted to a User for a Specified Project	×	iam:permissions:listRolesForUserOnProject	-	-
Querying All Permissions of a User Group	×	iam:permissions:listRolesForGroup	-	-
Checking Whether a User Group Has Specified Permissions	×	iam:permissions:checkRoleForGroup	-	-
Removing Permissions of a User Group	×	iam:permissions:revokeRoleFromGroup	-	-
Query Permission Assignment Records	×	iam:permissions:listRoleAssignments	-	-

Custom Policy Management

Permission	API	Action	IAM Project	Enterprise Project
Listing Custom Policies	**GET /v3.0/OS-ROLE/roles**	iam:roles:listRoles	-	-
Querying Custom Policy Details	**GET /v3.0/OS-ROLE/roles/{role_id}**	iam:roles:getRole	-	-
Creating a Custom Policy for Cloud Services	**POST /v3.0/OS-ROLE/roles**	iam:roles:createRole	-	-

Permission	API	Action	IAM Project	Enterprise Project
Modifying a Custom Policy for Cloud Services	**PATCH /v3.0/OS-ROLE/roles/{role_id}**	iam:roles:updateRole	-	-
Deleting a Custom Policy	**DELETE /v3.0/OS-ROLE/roles/{role_id}**	iam:roles:deleteRole	-	-

Agency Management

Permission	API	Action	IAM Project	Enterprise Project
Creating an Agency	**POST /v3.0/OS-AGENCY/agencies**	iam:agencies:createAgency	-	-
Listing Agencies	**GET /v3.0/OS-AGENCY/agencies**	iam:agencies:listAgencies	-	-
Querying Agency Details	**GET /v3.0/OS-AGENCY/agencies/{agency_id}**	iam:agencies:getAgency	-	-
Modifying an Agency	**PUT /v3.0/OS-AGENCY/agencies/{agency_id}**	iam:agencies:updateAgency	-	-
Deleting an Agency	**DELETE /v3.0/OS-AGENCY/agencies/{agency_id}**	iam:agencies:deleteAgency	-	-
Granting Permissions to an Agency for a Region-specific Project	**PUT /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}**	iam:permissions:grantRoleToAgencyOnProject	-	-
Checking Whether an Agency Has Specified Permissions for a Region-specific Project	**HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}**	iam:permissions:checkRoleForAgencyOnProject	-	-

Permission	API	Action	IAM Project	Enterprise Project
Querying Permissions of an Agency for a Region-specific Project	**GET /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles**	iam:permissions:listRolesForAgencyOnProject	-	-
Removing Permissions of an Agency for a Region-specific Project	**DELETE /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}**	iam:permissions:revokeRoleFromAgencyOnProject	-	-
Granting Permissions to an Agency for the Global Service Project	**PUT /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}**	iam:permissions:grantRoleToAgencyOnDomain	-	-
Checking Whether an Agency Has Specified Permissions for the Global Service Project	**HEAD /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}**	iam:permissions:checkRoleForAgencyOnDomain	-	-
Querying Permissions of an Agency for the Global Service Project	**GET /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles**	iam:permissions:listRolesForAgencyOnDomain	-	-
Removing Permissions of an Agency for the Global Service Project	**DELETE /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}**	iam:permissions:revokeRoleFromAgencyOnDomain	-	-
Querying All Permissions of an Agency	**GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects**	iam:permissions:listRolesForAgency	-	-
Checking Whether an Agency Has Specified Permissions	**HEAD /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects**	iam:permissions:checkRoleForAgency	-	-

Permission	API	Action	IAM Project	Enterprise Project
Granting Specified Permissions to an Agency	**PUT /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects**	iam:permissions:grantRoleToAgency	-	-
Removing Permissions of an Agency	**DELETE /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects**	iam:permissions:revokeRoleFromAgency	-	-

Enterprise Project Management

Permission	API	Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Querying User Groups Associated with an Enterprise Project	**GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups**	iam:permissions:listGroupsOnEnterpriseProject	-	√
Querying the Permissions of a User Group Associated with an Enterprise Project	**GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles**	iam:permissions:listRolesForGroupOnEnterpriseProject	-	√
Granting Permissions to a User Group Associated with an Enterprise Project	**PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}**	iam:permissions:grantRoleToGroupOnEnterpriseProject	-	√

Permission	API	Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Deleting the Permissions of a User Group Associated with an Enterprise Project	**DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}**	iam:permissions:revokeRoleFromGroupOnEnterpriseProject	-	√
Querying Enterprise Projects Associated with a User Group	**GET /v3.0/OS-PERMISSION/groups/{group_id}/enterprise-projects**	iam:permissions:listEnterpriseProjectsForGroup	-	√
Querying Enterprise Projects Directly Associated with a User	**GET /v3.0/OS-PERMISSION/users/{user_id}/enterprise-projects**	iam:permissions:listEnterpriseProjectsForUser	-	√
Listing Users Associated with an Enterprise Project	**GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users**	iam:permissions:listUsersForEnterpriseProject	-	√
Listing Roles of a User Associated with an Enterprise Project	**GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles**	iam:permissions:listRolesForUserOnEnterpriseProject	-	√
Granting Permissions to a User Associated with an Enterprise Project	**PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}**	iam:permissions:grantRoleToUserOnEnterpriseProject	-	√
Deleting Roles of a User Associated with an Enterprise Project	**DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}**	iam:permissions:revokeRoleFromUserOnEnterpriseProject	-	√

Security Settings

Permission	API	Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Modifying the Operation Protection Policy	**PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy**	iam:securitypolicies:updateProtectPolicy	-	-
Querying the Operation Protection Policy	**GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy**	iam:securitypolicies:getProtectPolicy	-	-
Modifying the Password Policy	**PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy**	iam:securitypolicies:updatePasswordPolicy	-	-
Querying the Password Policy	**GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy**	iam:securitypolicies:getPasswordPolicy	-	-
Modifying the Login Authentication Policy	**PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy**	iam:securitypolicies:updateLoginPolicy	-	-
Querying the Login Authentication Policy	**GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy**	iam:securitypolicies:getLoginPolicy	-	-
Modifying the ACL for Console Access	**PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy**	iam:securitypolicies:updateConsoleAclPolicy	-	-
Querying the ACL for Console Access	**GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy**	iam:securitypolicies:getConsoleAclPolicy	-	-
Modifying the ACL for API Access	**PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy**	iam:securitypolicies:updateApiAclPolicy	-	-

Permission	API	Action	IAM Project (Project)	Enterprise Project (Enterprise Project)
Querying the ACL for API Access	**GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy**	iam:securitypolicies:getApiAclPolicy	-	-

Federated Identity Authentication Management

Permission	API	Action	IAM Project	Enterprise Project
Listing Identity Providers	**GET /v3/OS-FEDERATION/identity_providers**	iam:identityProviders:listIdentityProviders	-	-
Querying Identity Provider Details	**GET /v3/OS-FEDERATION/identity_providers/{id}**	iam:identityProviders:getIdentityProvider	-	-
Creating a SAML Identity Provider	**PUT /v3/OS-FEDERATION/identity_providers/{id}**	iam:identityProviders:createIdentityProvider	-	-
Modifying a SAML Identity Provider	**PATCH /v3/OS-FEDERATION/identity_providers/{id}**	iam:identityProviders:updateIdentityProvider	-	-
Deleting a SAML Identity Provider	**DELETE /v3/OS-FEDERATION/identity_providers/{id}**	iam:identityProviders:deleteIdentityProvider	-	-
Creating an OpenID Connect Identity Provider	**POST /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config**	iam:identityProviders:createOpenIDConnectConfig	-	-
Modifying an OpenID Connect Identity Provider	**PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config**	iam:identityProviders:updateOpenIDConnectConfig	-	-
Querying Details About an OpenID Connect Identity Provider	**GET /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config**	iam:identityProviders:getOpenIDConnectConfig	-	-

Permission	API	Action	IAM Project	Enterprise Project
Listing Mappings	**GET /v3/OS-FEDERATION/mappings**	iam:identityProviders:listMappings	-	-
Querying Mapping Details	**GET /v3/OS-FEDERATION/mappings/{id}**	iam:identityProviders:getMapping	-	-
Registering a Mapping	**PUT /v3/OS-FEDERATION/mappings/{id}**	iam:identityProviders:createMapping	-	-
Updating a Mapping	**PATCH /v3/OS-FEDERATION/mappings/{id}**	iam:identityProviders:updateMapping	-	-
Deleting a Mapping	**DELETE /v3/OS-FEDERATION/mappings/{id}**	iam:identityProviders:deleteMapping	-	-
Listing Protocols	**GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols**	iam:identityProviders:listProtocols	-	-
Querying Protocol Details	**GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}**	iam:identityProviders:getProtocol	-	-
Registering a Protocol	**PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}**	iam:identityProviders:createProtocol	-	-
Updating a Protocol	**PATCH /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}**	iam:identityProviders:updateProtocol	-	-
Deleting a Protocol	**DELETE /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}**	iam:identityProviders:deleteProtocol	-	-

Permission	API	Action	IAM Project	Enterprise Project
Querying a Metadata File	**GET /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata**	iam:identityProviders:getIDPMetadata	-	-
Importing a Metadata File	**POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata**	iam:identityProviders:createIDPMetadata	-	-

8 Appendix

8.1 Status Codes

Table 8-1 Status codes

Status Code	Message Title	Description
100	Continue	The client should continue with its request. This interim response is used to inform the client that the initial part of the request has been received and has not yet been rejected by the server.
101	Switching Protocols	The requester has asked the server to switch protocols and the server has agreed to do so. The protocol should be switched only when it is advantageous to do so. For example, switching to a newer version of HTTP is advantageous over older versions.
201	Created	The request has been fulfilled and resulted in a new resource being created.
202	Accepted	The request has been accepted for processing, but the processing has not been completed.
203	Non-Authoritative Information	The server successfully processed the request, but is returning information that may be from another source.

Status Code	Message Title	Description
204	NoContent	The server successfully processed the request and is not returning any content. The status code is returned in response to an HTTP OPTIONS request.
205	Reset Content	The server successfully processed the request, but is not returning any content.
206	Partial Content	The server has fulfilled the partial GET request for the resource.
300	Multiple Choices	There are multiple options for the resource from which the client may choose. For example, this code could be used to present a list of resource characteristics and addresses from which the client such as a browser may choose.
301	Moved Permanently	The requested resource has been assigned a new permanent URI and any future references to this resource should use one of the returned URIs.
302	Found	The requested resource resides temporarily under a different URI.
303	See Other	The response to the request can be found under a different URI and should be retrieved using a GET or POST method.
304	Not Modified	The requested resource has not been modified. When the server returns this status code, it does not return any resources.
305	Use Proxy	The requested resource must be accessed through a proxy.
306	Unused	This HTTP status code is no longer used.
400	BadRequest	The request could not be understood by the server due to malformed syntax. The client should not repeat the request without modifications.
401	Unauthorized	The authorization information provided by the client is incorrect or invalid. Check the username and password.
402	Payment Required	This status code is reserved for future use.

Status Code	Message Title	Description
403	Forbidden	The server understood the request, but is refusing 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.
405	MethodNotAllowed	The method specified in the request is not allowed for the requested resource. The client should not repeat the request without modifications.
406	Not Acceptable	The server cannot fulfill the request based on the content characteristics of the request.
407	Proxy Authentication Required	This code is similar to 401, but indicates that the client must first authenticate itself with the proxy.
408	Request Time-out	The client does not produce a request within the time that the server was prepared to wait. The client may repeat the request without modifications at any later time.
409	Conflict	The request could not be completed due to a conflict with the current state of the resource. This status code indicates that the resource that the client attempts to create already exists, or the request fails to be processed because of the update of the conflict request.
410	Gone	The requested resource is no longer available. The requested resource has been deleted permanently.
411	Length Required	The server refuses to process the request without a defined Content-Length.
412	Precondition Failed	The server does not meet one of the preconditions that the requester puts on the request.

Status Code	Message Title	Description
413	Request Entity Too Large	The server is refusing to process a request because the request entity is larger than the server is willing or able to process. The server may close the connection to prevent the client from continuing the request. If the condition is temporary, the server should include a **Retry-After** header field to indicate that it is temporary and after what time the client may try again.
414	Request-URI Too Large	The server is refusing to service the request because the request URI is longer than the server is willing to interpret.
415	Unsupported Media Type	The server is refusing to service the request because the entity of the request is in a format not supported by the requested resource for the requested method.
416	Requested range not satisfiable	The requested range is invalid.
417	Expectation Failed	The server fails to meet the requirements of the **Expect** request header field.
422	UnprocessableEntity	The request was well-formed but was unable to be followed due to semantic errors.
429	TooManyRequests	The client has sent more requests than its rate limit is allowed within a given amount of time, or the server has received more requests than it is able to process within a given amount of time. In this case, the client should repeat requests after the time specified in the **Retry-After** header of the response expires.
500	InternalServerError	The server encountered an unexpected condition which prevented it from fulfilling the request.
501	Not Implemented	The server does not support the functionality required to fulfill the request.
502	Bad Gateway	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.
503	ServiceUnavailable	The requested service is unavailable. The client should not repeat the request without modifications.

Status Code	Message Title	Description
504	ServerTimeout	The request cannot be fulfilled within a given amount of time. The response will reach the client only if the request carries a timeout parameter.
505	HTTP Version not supported	The server does not support the HTTP protocol version used in the request.

8.2 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 **Error Codes**.

Status Code	Error Code	Error Message	Description	Measure
400	1100	Mandatory parameters are not specified.	Mandatory parameters are not specified.	Check the request parameters.
400	1101	Invalid username.	Invalid username.	Check the username.
400	1102	Invalid email address.	Invalid email address.	Check the email address.
400	1103	Incorrect password.	Incorrect password.	Check the password.
400	1104	Invalid mobile number.	Invalid mobile number.	Check the mobile number.
400	1105	The value of **xuser_type** must be the same as that of **xdomain_type**.	The value of **xuser_type** must be the same as that of **xdomain_type**.	Check whether the value of **xuser_type** is the same as that of **xdomain_type**.
400	1106	The country code and mobile number must be set at the same time.	The country code and mobile number must be set at the same time.	Check whether the country code and mobile number have been both specified.

Status Code	Error Code	Error Message	Description	Measure
400	1107	The account administrator cannot be deleted.	The account administrator cannot be deleted.	This operation is not allowed.
400	1108	The new password must be different from the old password.	The new password must be different from the old password.	Enter another password.
400	1109	The username already exists.	The username already exists.	Modify the username.
400	1110	The email address has already been used.	The email address has already been used.	Enter another email address.
400	1111	The mobile number has already been used.	The mobile number has already been used.	Enter another mobile number.
400	1113	The values of **xuser_id** and **xuser_type** already exist.	The values of **xuser_id** and **xuser_type** already exist.	Modify the values of **xuser_id** and **xuser_type**.
400	1115	The number of IAM users has reached the maximum allowed limit.	The number of IAM users has reached the maximum allowed limit.	Modify the user quota or contact technical support.
400	1117	Invalid user description.	Invalid user description.	Modify the user description.
400	1118	The password is weak.	The password is weak.	Enter another password.
400	IAM.0007	Request parameter %(key)s is invalid.	The request parameter is invalid.	Check the request parameter.
400	IAM.0008	Please scan the QR code first.	Scan the QR code first.	Scan the QR code first.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.0009	X-Subject-Token is invalid in the request.	**X-Subject-Token** in the request is invalid.	Check the request parameter.
400	IAM.0010	The QR code has already been scanned by another user.	The QR code has already been scanned by someone else.	No action is required.
400	IAM.0011	Request body is invalid.	The request body is invalid.	Check the request body.
400	IAM.0072	'%(key)s' is a required property.	The request is invalid. For example, %(key)s is required.	Contact technical support.
400	IAM.0073	Invalid input for field '%(key)s'. The value is '%(value)s'.	The input is invalid.	Contact technical support.
400	IAM.0077	Invalid policy type.	The policy type is invalid.	Contact technical support.
400	IAM.1000	The role must be a JSONObject.	The role object is missing.	Check whether the request body contains the role object.
400	IAM.1001	The display_name must be a string and cannot be left blank or contain spaces.	The value of **display_name** is empty or contains spaces.	Check whether the value of **display_name** is correct.
400	IAM.1002	The length [input length] of the display name exceeds 64 characters.	The **display_name** field cannot exceed 64 characters.	Check the length of the **display_name** field.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.1003	The display_name contains invalid characters.	The **display_name** field contains invalid characters.	Check whether the value of **display_name** is correct.
400	IAM.1004	The type must be a string and cannot be left blank or contain spaces.	The **type** field is empty.	Check whether the value of **type** is correct.
400	IAM.1005	Invalid type [input type].	The **type** field is invalid.	Check whether the value of **type** is correct.
400	IAM.1006	The custom policy does not need a catalog.	Custom policies cannot contain the **catalog** field.	Delete the **catalog** field.
400	IAM.1007	The custom policy does not need a flag.	Custom policies cannot contain the **flag** field.	Delete the **flag** field.
400	IAM.1008	The custom policy does not need a name.	Custom policies cannot contain the **name** field.	Delete the **name** field.
400	IAM.1009	The type of a custom policy must be 'AX' or 'XA'.	The type of a custom policy can only be **AX** or **XA**.	Change the value of the **type** field to **AX** or **XA**.
400	IAM.1010	The catalog must be a string.	The value of the **catalog** field must be a character string.	Check whether the value of **catalog** is correct.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.1011	The length [input length] of the catalog exceeds 64 characters.	The **catalog** field cannot exceed 64 characters.	Check the length of the **catalog** field.
400	IAM.1012	Invalid catalog.	The **catalog** field is invalid.	Check whether the value of **catalog** is correct.
400	IAM.1013	The flag must be a string.	The value of the **flag** field must be a character string.	Check whether the value of **flag** is correct.
400	IAM.1014	The value of the flag must be 'fine_grained'.	The value of **flag** is not **fine_grained**.	Change the value of **flag** to **fine_grained**.
400	IAM.1015	The name must be a string and cannot be left blank or contain spaces.	The **name** field is empty.	Specify the **name** field for system-defined roles.
400	IAM.1016	The length of the name [input name] cannot exceed 64 characters.	The value of **name** cannot exceed 64 characters.	Check whether the value of **name** is correct.
400	IAM.1017	Invalid name.	The **name** field is invalid.	Check whether the value of **name** is correct.
400	IAM.1018	Invalid description.	The **description** field is invalid.	Check whether the value of **description** is correct.
400	IAM.1019	Invalid description_cn.	The **description_cn** field is invalid.	Check whether the value of **description_cn** is correct.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.1020	The policy must be a JSONObject.	The **policy** object is missing.	Check whether the request body contains the **policy** object.
400	IAM.1021	The size [input policySize] of the policy exceeds 6,144 characters.	The **policy** object contains more than 6144 characters.	Check the length of the **policy** object.
400	IAM.1022	The length [input id length] of the ID exceeds 128 characters.	The **id** field contains more than 128 characters.	Check the length of the **id** field.
400	IAM.1023	Invalid ID '[input id]'.	The **id** field of the policy is invalid.	Check whether the value of **id** is correct.
400	IAM.1024	The version of a fine-grained policy must be '1.1'.	The version of the fine-grained policy is not 1.1.	Change the value of **version** to **1.1**.
400	IAM.1025	Fine-grained policies do not need depends.	The fine-grained policy contains the **depends** field.	Delete the **depends** field.
400	IAM.1026	The version of an RBAC policy must be '1.0' or '1.1'.	The version of an RBAC policy can only be 1.0 or 1.1.	Change the value of **version** to **1.0** or **1.1**.
400	IAM.1027	The Statement/ Rules must be a JSONArray.	The **statement** field is not a JSON array.	Check whether a JSON array statement exists.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.1028	The number of statements [input statement size] must be greater than 0 and less than or equal to 8.	The policy does not contain any statements or contains more than 8 statements.	Ensure that the policy contains 1 to 8 statements.
400	IAM.1029	The value of Effect must be 'allow' or 'deny'.	The value of **effect** can only be **allow** or **deny**.	Set the **effect** field to **allow** or **deny**.
400	IAM.1030	The Action or NotAction must be a JSONArray.	The **action** or **notAction** field is invalid.	Check whether the value of **action** is correct.
400	IAM.1031	The Action and NotAction cannot be set at the same time in a statement.	The **action** and **notAction** fields cannot exist at the same time.	Delete the **action** or **notAction** field.
400	IAM.1032	The OCP NotAction cannot be 'allow'.	The **notAction** field cannot be **allow** for organization control policies (OCPs).	Specify the **notAction** field as **deny** for OCP policies.
400	IAM.1033	The number of actions [input action size] exceeds 100.	The number of actions exceeds 100.	Ensure that the number of actions does not exceed 100.
400	IAM.1034	The length [input urn length] of an action URN exceeds 128 characters.	An action contains more than 128 characters.	Ensure that each action does not exceed 128 characters.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.1035	Action URN '[input urn]' contains invalid characters.	The action contains invalid characters.	Check whether the value of **action** is correct.
400	IAM.1036	Action '[input action]' has not been registered.	The action has not been registered.	Register the action using APIs of the registration center.
400	IAM.1037	The number of resource URIs [input Resource uri size] must be greater than 0 and less than or equal to 20.	Only 1 to 20 resources are allowed.	Check the number of resources.
400	IAM.1038	Resource URI '[input resource uri]' is invalid. Old resources only support agencies.	The resource URI is invalid.	Check whether each resource URI is correct.
400	IAM.1039	Old policies do not support conditions.	Old policies cannot contain the **condition** field.	Delete the **condition** field or use the new policy format.
400	IAM.1040	The number of resources [input Resource size] must be greater than 0 and less than or equal to 10.	Only 1 to 10 resource URIs are allowed.	Check the number of URIs of each resource object.
400	IAM.1041	The resource URI cannot be left blank or contain spaces.	A resource URI is empty.	Check whether each resource URI is correct.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.1042	The length [input uri length] of a resource URI exceeds 1,500 characters.	A resource URI contains more than 1,500 characters.	Check the length of each resource URI.
400	IAM.1043	A region must be specified.	A region must be specified.	Specify a region in the resource URI.
400	IAM.1044	Region '[input resource region]' of resource '[input resource]' is invalid.	The **region** field is invalid.	Check whether the value of **region** is correct.
400	IAM.1045	Resource URI '[input resource uri]' or service '[input resource split]' is invalid.	The service name in the resource URI is invalid.	Check whether the service name is correct or register the service first.
400	IAM.1046	Resource URI '[input resource]' or resource type '[input resource split]' is invalid.	The resource type in the resource URI is invalid.	Check whether the resource type is correct or register the resource type first.
400	IAM.1047	Resource URI '[input resource uri]' contains invalid characters.	The resource URI is invalid.	Check whether the resource URI is correct.
400	IAM.1048	Resource URI '[input resource uri]' is too long or contains invalid characters.	The resource URI contains invalid characters.	Check whether the **id** field contains invalid characters.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.1049	The Resource must be a JSONObject or JSONArray.	The **resource** object is missing.	Check whether the **resource** object is a JSON array.
400	IAM.1050	The number of conditions [input condition size] must be greater than 0 and less than or equal to 10.	Only 1 to 10 conditions are allowed.	Specify at least one condition or delete unused conditions.
400	IAM.1051	The values of Operator '[input operator]' cannot be null.	No operator is specified.	Enter a correct operator.
400	IAM.1052	Invalid Attribute '[input attribute]'.	The attribute is invalid.	Check the attribute value.
400	IAM.1053	Attribute '[input attribute]' must be a JSONArray.	The attribute is not a JSON array.	Check whether the attribute object is a JSON array.
400	IAM.1054	The number [input attribute size] of attributes '[input attribute]' for operator '[input operator]' must be greater than 0 and less than or equal to 10.	Each operator can only be used together with 1 to 10 attributes.	Check whether the number of attributes for each operator is correct.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.1055	Attribute '[input attribute]' does not match operator '[input operator]'.	The attribute does not match the operator.	Check whether the attribute and operator match.
400	IAM.1056	The length [condition length] of attribute '[input attribute]' for operator '[input operator]' must be greater than 0 and less than or equal to 1024 characters.	Each condition can contain only 1 to 1024 characters.	Check the total length of the **condition** object.
400	IAM.1057	Value [input condition] of attribute [input attributes] for operator [input operator] contains invalid characters.	The **condition** field contains invalid characters.	Check whether the **condition** field contains invalid characters.
400	IAM.1058	The number of depends [input policyDepends size] exceeds 20.	The number of dependent permissions exceeds 20.	Delete excessive dependent permissions.
400	IAM.1059	Invalid key '{}'.	The policy contains an invalid key.	Modify or delete the invalid key in the policy request body.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.1060	The value of key '{}' must be a string.	The value of this field must be a character string.	Change the values of **display_name** and **name** to character strings.
400	IAM.1061	Invalid TOTP passcode.	The authenticatio n key is invalid.	Check the request or contact technical support.
400	IAM.1062	Login protection has been bound to mfa, the unbinding operation cannot be performed.	Login protection has been enabled and requires virtual MFA device based verification. You cannot unbind the virtual MFA device.	Check the request or contact technical support.
400	IAM.1101	The request body size %s is invalid.	The size of the request body does not meet the requirements.	Check whether the request body is empty or larger than 32 KB.
400	IAM.1102	The %s in the request body is invalid.	The value in the request body is incorrect.	Check the attribute value in the request body by referring to the *API Reference*.
400	IAM.1103	The %s is required in the request body.	The parameter is required but not specified in the request body.	Check the request body by referring to the *API Reference*.
400	IAM.1104	The access key %s is in the blacklist.	The AK in the request has been blacklisted.	Check whether the AK exists.
400	IAM.1105	The access key %s has expired.	The AK in the request has expired.	Create a new access key.

Status Code	Error Code	Error Message	Description	Measure
400	IAM.1106	The user %s with access key %s cannot be found.	The AK does not have matching user information.	Check whether the user or agency corresponding to the AK exists.
400	IAM.1107	The access key %s is inactive.	The AK in the request has been disabled.	Enable the AK.
400	IAM.1108	The securitytoken has expired.	The temporary access key has expired.	Obtain a new temporary access key.
400	IAM.1109	The project information cannot be found.	No project information can be found.	Check whether the project specified in the request body or token exists. If the fault persists, contact technical support.
401	IAM.0001	The request you have made requires authentication.	Authentication failed.	Complete or check the authentication information.
401	IAM.0061	Account locked.	The user has been locked.	Wait until the user is unlocked.
401	IAM.0062	Incorrect password.	Incorrect password.	Enter the correct password.
401	IAM.0063	Access token authentication failed.	Access token authentication failed.	Contact technical support.
401	IAM.0064	The access token does not have permissions for the request.	The IAM user does not have the required permissions.	Check the permissions of the IAM user.

Status Code	Error Code	Error Message	Description	Measure
401	IAM.0065	HUAWEI IDs registered in European countries cannot log in to HUAWEI CLOUD.	HUAWEI ID login is not supported in European sites.	Log in using a supported account.
401	IAM.0066	The token has expired.	The token has expired.	Use a valid token.
401	IAM.0067	Invalid token.	Invalid token.	Enter a valid token.
403	IAM.0002	You are not authorized to perform the requested action.	You do not have permission to perform this action.	Check whether you have been granted the permissions required to perform this action.
403	IAM.0003	Policy doesn't allow %(actions)s to be performed.	The action is not allowed in the policy.	Check whether the action is allowed in the policy.
403	IAM.0080	The user %s with access key %s is disabled.	The user corresponding to the AK has been disabled.	Contact the security administrator of the user.
403	IAM.0081	This user only supports console access, not programmatic access.	The user only has access to the management console.	Contact the security administrator of the user to change the user's access type.
403	IAM.0082	The user %s is disabled.	The user is disabled.	Contact the security administrator of the user.
403	IAM.0083	You do not have permission to access the private region %s.	You do not have permission to access private regions.	Select another region or contact the private region administrator.

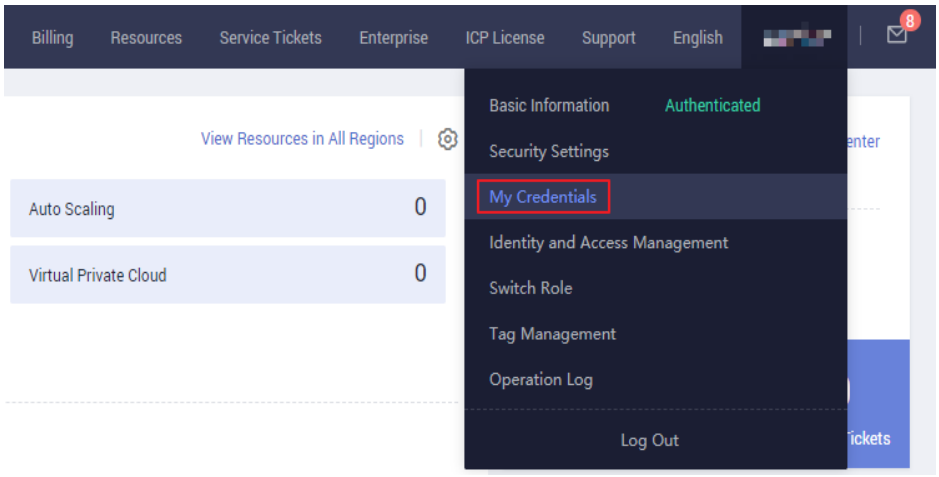
Status Code	Error Code	Error Message	Description	Measure
404	IAM.0004	Could not find % (target)s: % (target_id)s.	The requested resource cannot be found.	Check the request or contact technical support.
409	IAM.0005	Conflict occurred when attempting to store % (type)s - % (details)s.	A conflict occurs when the requested resource is saved.	Check the request or contact technical support.
410	IAM.0020	Original auth failover to other regions, please auth downgrade	The Auth service in the original region is faulty and has switched to another region.	The system will automatically downgrade the authentication. No action is required.
429	IAM.0012	The throttling threshold has been reached. Threshold: %d times per %d seconds	The throttling threshold has been reached.	Check the request or contact technical support.
500	IAM.0006	An unexpected error prevented the server from fulfilling your request.	A system error occurred.	Contact technical support.

8.3 Obtaining Account, IAM User, Group, Project, Region, and Agency Information

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**.

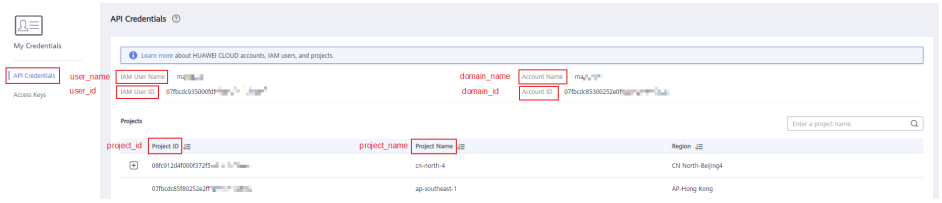
Figure 8-1 My Credentials



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 8-2 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 to which the project belongs.

----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

A Change History

Table A-1 Change History

Released On	Description
2023-09-14	This issue is the second official release, which incorporates the following changes: • Added **Granting Permissions to Agencies Associated with Specified Enterprise Projects**. • Added **Removing Permissions of Agencies Associated with Specified Enterprise Projects**.
2022-09-30	This issue is the first official release.

