Identity and Access Management

User Guide

Issue 22

Date 2025-07-03

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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Before You Start

Intended Audience

The Identity and Access Management (IAM) service is intended for administrators, including:

- Account administrator (with full permissions for all services, including IAM)
- IAM users added to the **admin** group (with full permissions for all services, including IAM)
- IAM users assigned the **Security Administrator** role (with permissions to access IAM)

If you want to view, audit, and track the records of key operations performed on IAM, enable Cloud Trace Service (CTS). For details, see **Key IAM Operations Supported by CTS**.

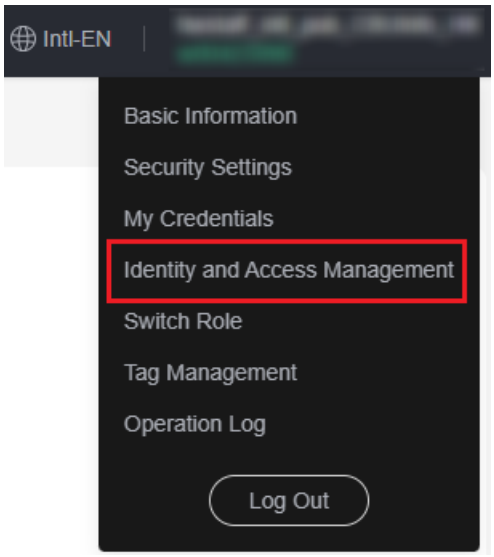
Accessing the IAM Console

Step 1 Log in to Huawei Cloud and click **Console** in the upper right corner.

Figure 1-1 Accessing the console

Step 2 On the management console, hover over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.

Figure 1-2 Accessing the IAM console



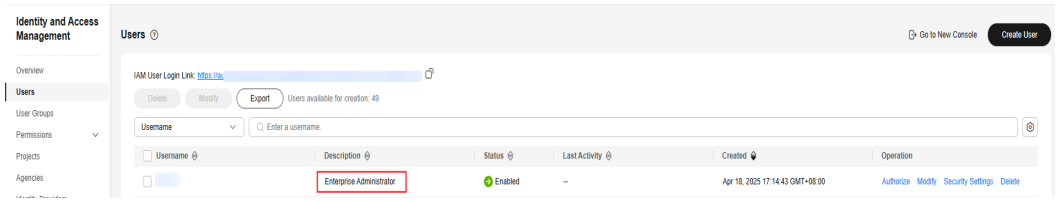
----End

Account

An account is created after you successfully register with Huawei Cloud. Your account owns resources and pays for the use of these resources. It has full access permissions for your resources. You cannot modify or delete your account in IAM, but you can do so in My Account.

After you log in to your account, you will see a user marked **Enterprise administrator** on the **Users** page of the IAM console.

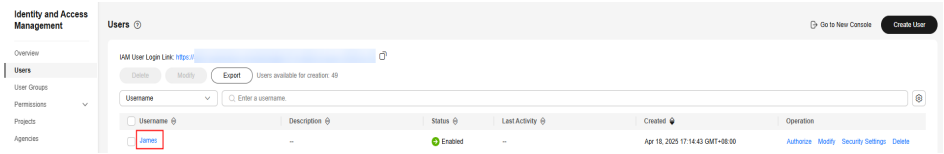
Figure 1-3 IAM user corresponding to the account



IAM User

You can create users in IAM as the administrator and assign permissions for specific resources. As shown in the following figure, **James** is an IAM user created by the administrator. IAM users can log in to Huawei Cloud using their account name, usernames, and passwords, and then use resources based on the assigned permissions. IAM users do not own resources and cannot make payments. You can use your account to pay for the resources they use.

Figure 1-4 IAM user created by the administrator

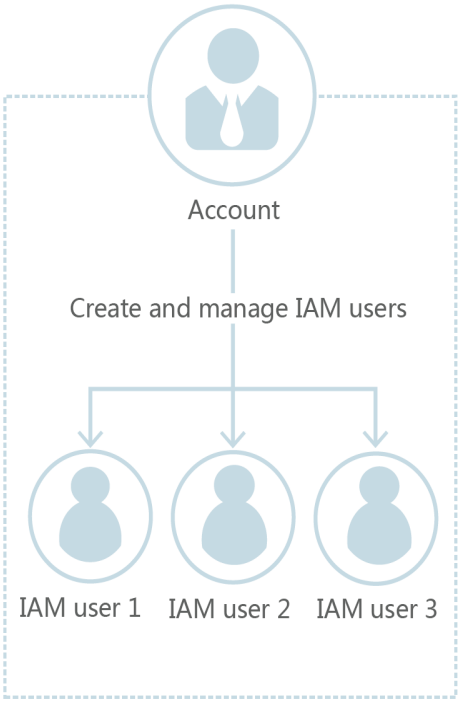


Relationship Between an Account and Its IAM Users

An account and its IAM users have a parent-child relationship. The account owns the resources and makes payments for the resources used by IAM users. It has full permissions for these resources.

IAM users are created by the account administrator, and only have the permissions granted by the administrator. The administrator can modify or revoke the IAM users' permissions at any time. Resources used by IAM users in your account are billed to your account. IAM users do not need to make payments themselves.

Figure 1-5 Relationship between an account and its IAM users

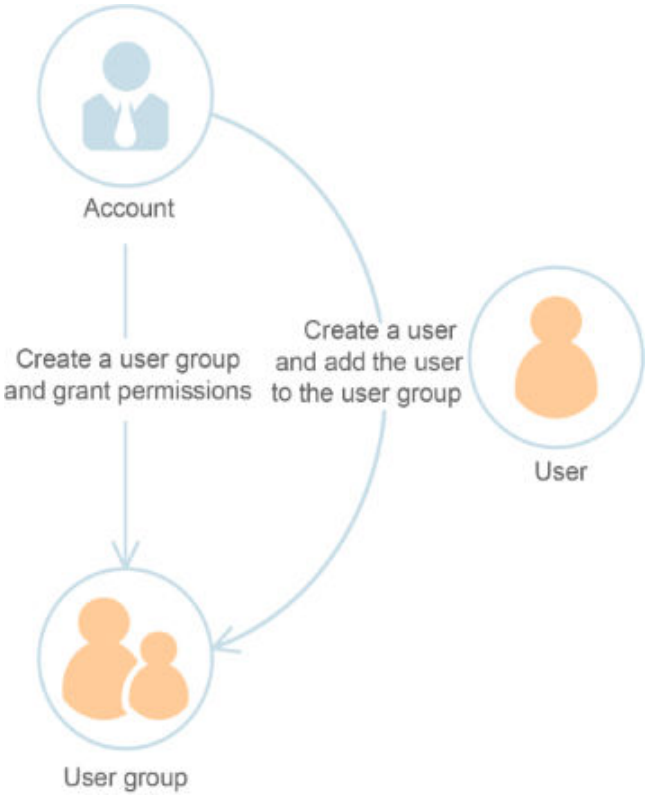


User Group

You can use user groups to assign permissions to IAM users. After an IAM user is added to a user group, the user has the permissions of the group and can perform operations on cloud services as specified by the permissions. If a user is added to multiple user groups, the user inherits the permissions assigned to all these groups.

The default user group **admin** has all permissions required to use all of the cloud resources. Users in this group can perform operations on all the resources, including but not limited to creating user groups and users, modifying permissions, and managing resources.

Figure 1-6 User group



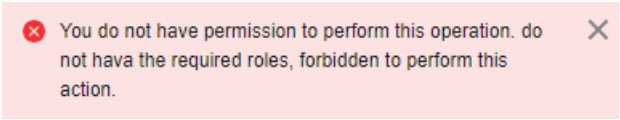
Permission

IAM provides common permissions for different services, such as administrator and read-only permissions. New IAM users do not have any permissions assigned by default. The administrator must add them to one or more groups and attach permissions policies or roles to these groups so that the IAM users can inherit permissions from the groups. IAM users can also assign permissions to themselves. Then the IAM users can perform specific operations on cloud services.

- Roles: A coarse-grained authorization strategy that defines permissions by job responsibility. Only a limited number of service-level roles are available for authorization. Cloud services often depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.
- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only permission to manage a certain type of Elastic Cloud Servers (ECSs).

When an IAM user granted only ECS permissions accesses other services, a message similar to the following will be displayed.

Figure 1-7 No permissions

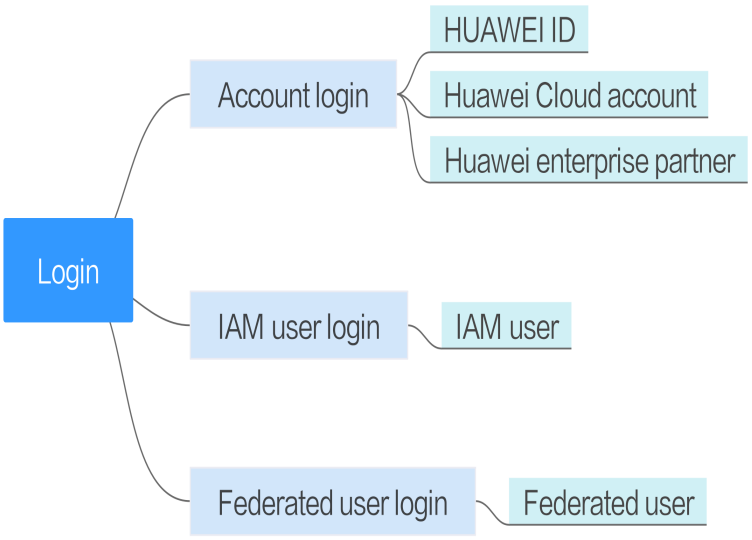


2 Logging In to Huawei Cloud

You can log in to Huawei Cloud using any of the following methods (see **Figure 2-1**):

- **Account login**: Log in with the account that was created when you use Huawei Cloud. Your account has full access permissions for your resources and makes payments for the use of these resources. To log in to Huawei Cloud using an account, do as follows:
  - **HUAWEI ID**: A HUAWEI ID is a unified identity that you can use to access all Huawei services. It is **different from a Huawei Cloud account**. Ensure that you have already registered a HUAWEI ID. If you do not have a HUAWEI ID, create one and use it to enable Huawei Cloud services. For details, see **Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services**.
  - **Huawei Cloud account**: Use your Huawei Cloud account to log in. If this is the first time you use Huawei Cloud, **register a HUAWEI ID and enable Huawei Cloud services**.
  - **Huawei Enterprise Partner Account**: When logging in using a Huawei enterprise partner account for the first time, associate these accounts with an existing or a new Huawei Cloud account. At the next login, you can directly log in using the Huawei website account or Huawei enterprise partner account. Alternatively, you can use the Huawei Cloud account to log in.
- **IAM user login**: IAM users are created by an **administrator** to use specific cloud services.
  - **IAM user**: **An account and IAM users** have a parent-child relationship. IAM users can only use specific cloud services based on assigned permissions.
- **Federated user login**: Federated users are registered with an enterprise IdP that is created by the **administrator** in IAM.
  - **Federated user**: You can log in to Huawei Cloud as a federated user if you have obtained the name of the identity provider, the Huawei Cloud account used to create this identity provider, and the username and password for logging in to your enterprise management system.

Figure 2-1 Logging in to Huawei Cloud



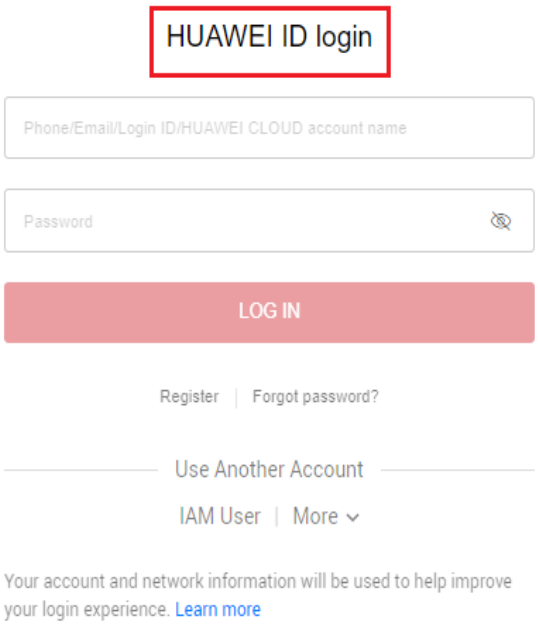
Logging In Using a HUAWEI ID

A HUAWEI ID is a unified identity that you can use to access all Huawei services. You can register and manage a HUAWEI ID on the **HUAWEI ID website**. You can also **register a HUAWEI ID and use it to enable Huawei Cloud services** in Huawei Cloud. When logging in to the Huawei Cloud console using a HUAWEI ID, you can enter a mobile number, email address, login ID, or Huawei Cloud account name.

To log in using a HUAWEI ID, do as follows:

Step 1 On the login page, enter your mobile number, email address, login ID, or Huawei Cloud account name, enter the password, and then click **LOG IN**.

Figure 2-2 Logging in using a HUAWEI ID



NOTE

- You can enter a Huawei Cloud account or a HUAWEI ID that has been used to enable Huawei Cloud services.
- If you enter a HUAWEI ID whose mobile number or email address has been used to enable Huawei Cloud services, go to **Step 2**.
- If you enter a HUAWEI ID whose mobile number or email address has not been used to enable Huawei Cloud services, go to **Step 3**.

Step 2 Select the account you want to use for login.

If the mobile number or email address you entered has been used to register a HUAWEI ID and Huawei Cloud account, select an account for login.

- Select the HUAWEI ID and click **OK**. Then, go to **Step 3**.
- Select the Huawei Cloud account and click **OK**. The login is successful.

Step 3 Click **Get code**, enter the verification code, and click **OK**.

If you have already associated both a mobile number and email address with your HUAWEI ID, you can choose mobile number or email address verification.

Step 4 In the **Trust this browser?** dialog box, click **TRUST**.

Step 5 In the displayed dialog box, click **Enable Huawei Cloud Services** or **Use Another Huawei Cloud Account**.

- **Enable Huawei Cloud Services**: Click this button to enable Huawei Cloud services for the HUAWEI ID so that you can use the HUAWEI ID to log in to Huawei Cloud. After clicking this button, go to **Step 6**.

- **Use Another Huawei Cloud Account**: Click this button to log in using another Huawei Cloud account. After clicking this button, go to **Step 1**.

Step 6 (Optional) If the mobile number or email address you entered has been used to register for Huawei Cloud accounts, select an account, and associate it with your HUAWEI ID.

NOTE

After you associate a Huawei Cloud account with your HUAWEI ID, you can use the HUAWEI ID to access Huawei Cloud, HUAWEI Developers, VMALL, and other Huawei services.

- Associating a Huawei Cloud account with your HUAWEI ID
  a. Select a Huawei Cloud account and click **Next**.
  b. Enter the password of the Huawei Cloud account and click **Next**.
  c. Confirm the HUAWEI ID information and click **OK**.
  d. Click **OK**. The Huawei Cloud homepage is displayed.

     NOTE

     - After you perform the preceding steps, your Huawei Cloud account is associated with your HUAWEI ID and becomes invalid. You need to use the HUAWEI ID for the next login.
     - If the upgrade fails, see "What Can I Do If the Upgrade to a HUAWEI ID Fails?" in the *IAM FAQs*.
- Enabling Huawei Cloud services

  Click **Skip This Step and Enable Huawei Cloud Services**, and go to **Step 7**.

Step 7 On the **Enable Huawei Cloud Services** page, read the service agreements and confirm that you accept them, and then click **Enable**.

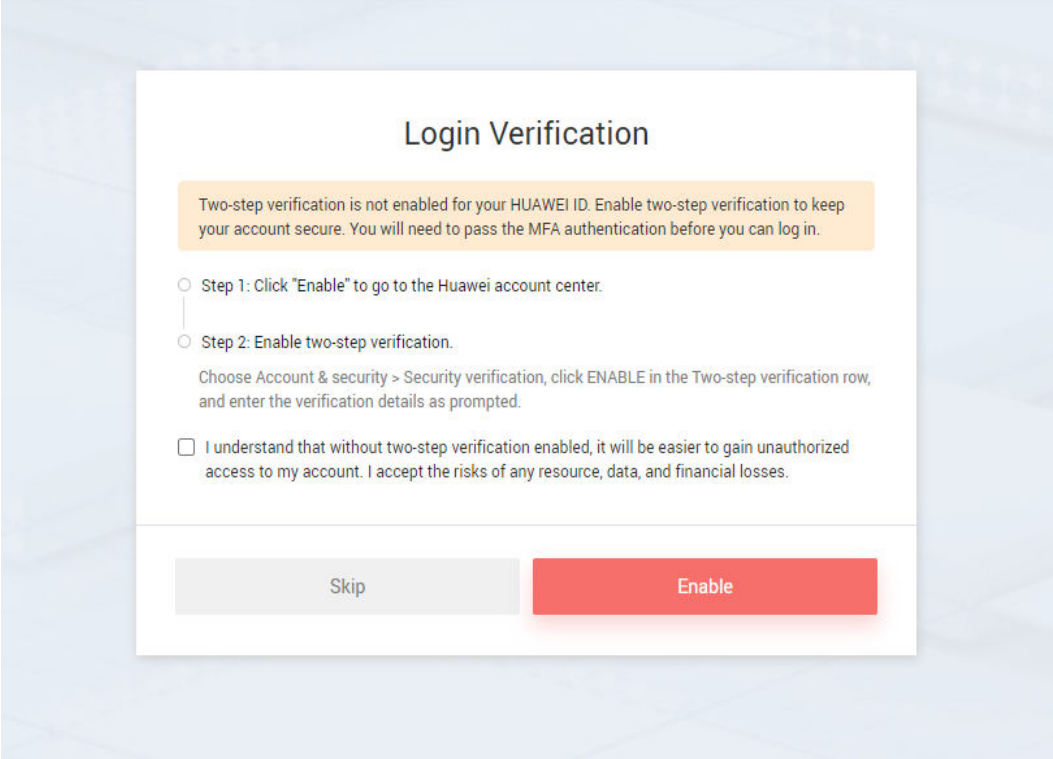
You can now use the HUAWEI ID to log in to Huawei Cloud.

Step 8 Verify the login. If two-step verification is not enabled for your HUAWEI ID, you will be directed to the login verification reminder page after logging in using the HUAWEI ID. The system will suggest enabling two-step verification. If you prefer not to enable it, click the checkbox to confirm and click **Skip** to directly access the Huawei Cloud management console.

Enable two-step verification

1. On the login verification page, click **Enable**.

Figure 2-3 Login verification



2. Choose **Account & security** > **Security verification**, click **ENABLE** in the **Two-step verification** row, and enter the verification details as prompted.

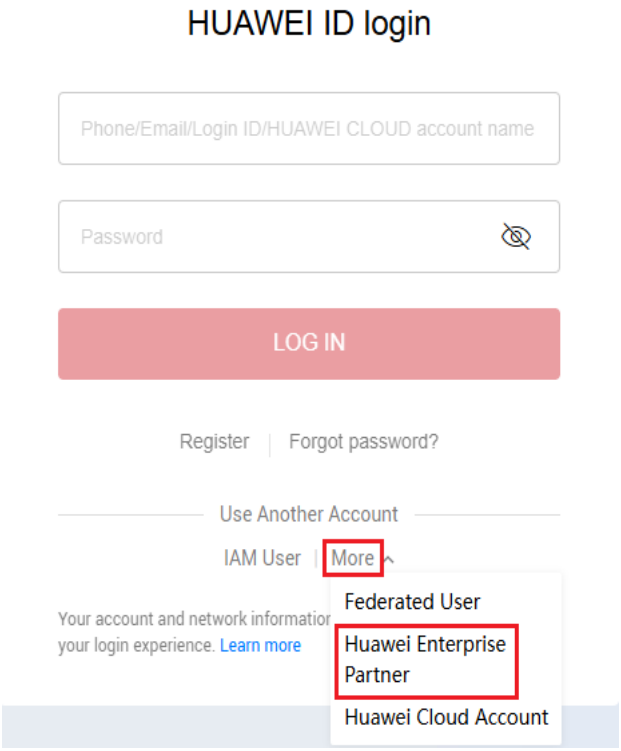
----End

Logging In Using a Huawei Enterprise Partner Account

If you already have a **Huawei enterprise partner account**, you can use them to log in to Huawei Cloud without additional credentials.

Step 1 On the login page, choose **More** > **Huawei Enterprise Partner**.

Figure 2-4 Logging in using a Huawei enterprise partner account



Step 2 Follow the prompts to log in to the Huawei enterprise partner account.

- If this is the first login, you will be requested to bind your Huawei website account to an existing or a new Huawei Cloud account. To create a new Huawei Cloud account, enter the account name, mobile number, and verification code. Click **Create and Bind**.
- If this is not the first login, you can directly log in using your Huawei website account.

Next time you log in to the Huawei Cloud console, you can use the name or mobile number set in step **Step 2** for the Huawei Cloud account.

----End

Logging In Using a Huawei Cloud Account

If you have a Huawei Cloud account, you can use it to log in to Huawei Cloud. The account owns resources you purchase, makes payments for the use of these resources, and has full access permissions for them. You can use the account to reset user passwords and assign permissions. When using the account to log in to the Huawei Cloud console, you can choose account/email login or mobile number login.

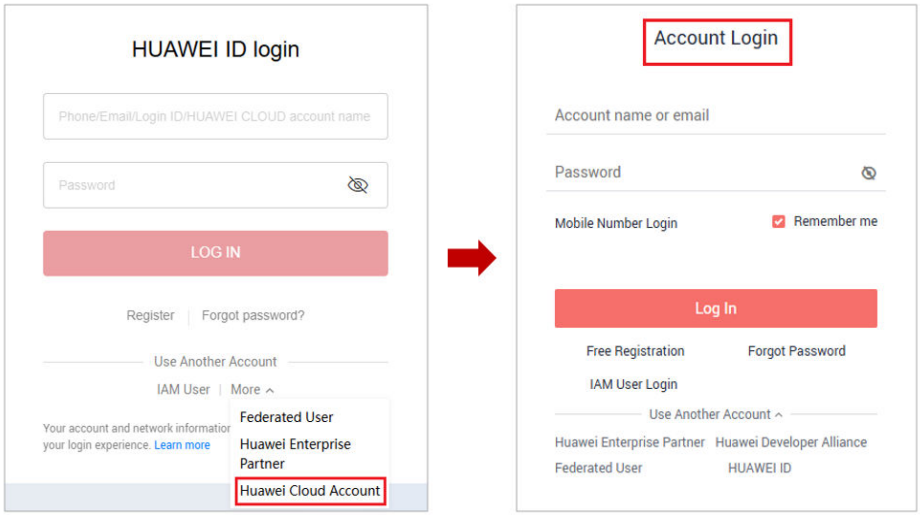
NOTE

If your Huawei Cloud account has been upgraded to a HUAWEI ID, use the HUAWEI ID to log in. For details, see **Logging In Using a HUAWEI ID**.

To log in using a Huawei Cloud account, do as follows:

Step 1 On the login page, click **Huawei Cloud Account**.

Figure 2-5 Logging in using a Huawei Cloud account



Step 2 Enter your account information and click **Log In**.

- **Account name or email**: The account name or the email address associated with the account.

  NOTE

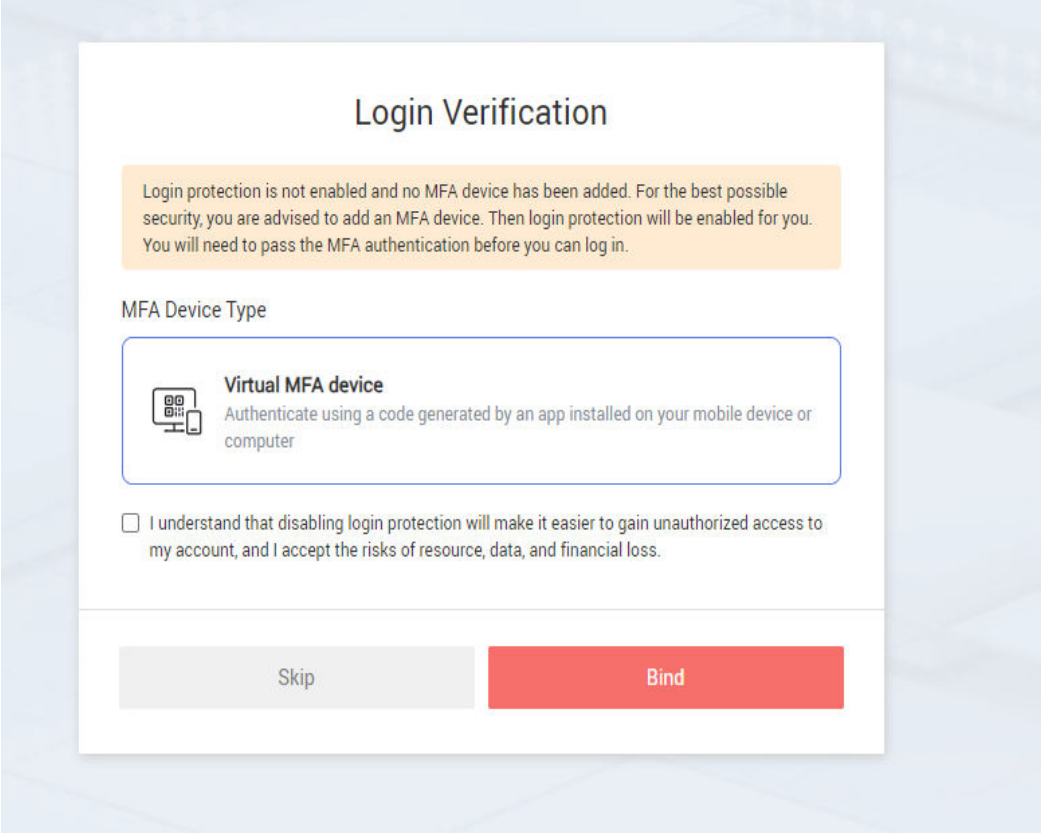
  Account names are case-insensitive.

- **Password**: The login password of the account. If you have forgotten your login password, **reset** it on the login page.
- **Mobile Number Login**: If you have forgotten the account name, click **Mobile Number Login**, and enter the associated mobile number and the login password to log in.

Step 3 Verify the login.

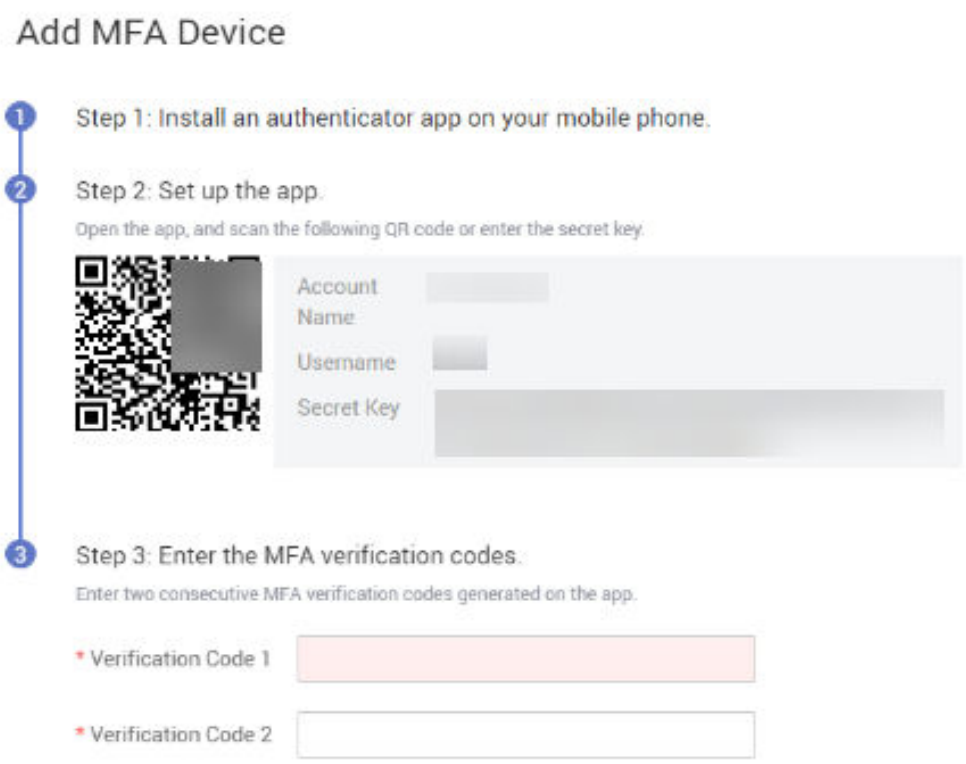
1. If login protection is not enabled for your Huawei Cloud account or no MFA device is added, you will be directed to a login verification page that suggests binding an MFA device. If you prefer not to bind it, click the confirmation checkbox and click **Skip** to directly access the Huawei Cloud management console.
   - **Binding a virtual MFA device**
     i. In the login verification dialog box, click **Bind**.

Figure 2-6 Login verification



ii. On the **Add MFA Device** page, enter the device name and type, then click **Next** to add a user to your MFA application.

Figure 2-7 Adding an MFA device



Add an MFA device by scanning the QR code or entering the secret key. The Huawei Cloud App is used as an example to describe how to add a user in an MFA application.

- Scanning the QR code

Open the MFA application and scan the QR code displayed on the **Bind Virtual MFA Device** page. Then the user is added to the MFA application.

- Entering the secret key

  Open the MFA application on your mobile phone, and enter the secret key.

  NOTE

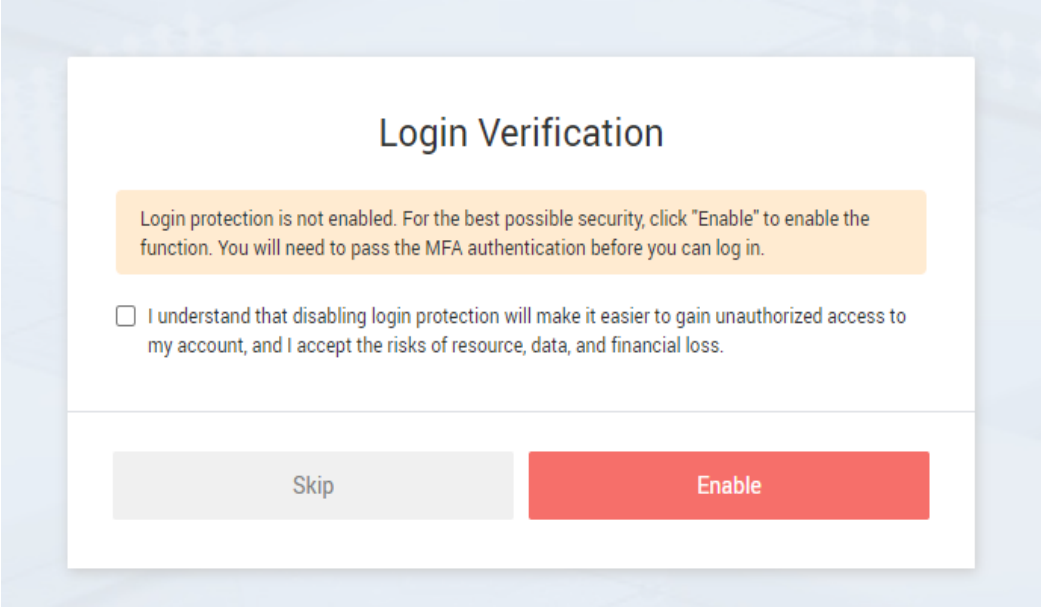
  The user can be manually added only using time-based one-time passwords (TOTP). You are advised to enable automatic time setting on your mobile device.

iii. After a user is added, go to the MFA application to view the verification codes. The code is automatically updated every 30 seconds.

iv. On the **Bind Virtual MFA Device** page, enter two consecutive verification codes and click **OK**. After a virtual MFA device is bound to your account, you can access the Huawei Cloud management console.

2. If login protection is not enabled for your Huawei Cloud account and an MFA device has been added, you will be directed to a verification page that suggests enabling login protection. If you prefer not to enable it, select the confirmation checkbox and click **Skip** to directly access the Huawei Cloud management console.
   - **Enabling login protection**
     i. On the login verification page, click **Enable** to enter the MFA authentication page.

     Figure 2-8 Login verification

     ii. Enter the virtual MFA dynamic code, then click **OK** to access the Huawei Cloud management console.

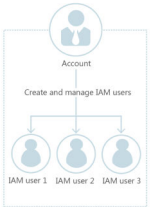
----End

Logging In as an IAM User

IAM users can be created using your Huawei Cloud account or by an **administrator**. Each IAM user has their own identity credentials (password and access keys) and uses cloud resources based on assigned permissions. IAM users cannot make payments themselves. You can use your account to pay for the resources they use.

Your account and IAM users have a parent-child relationship.

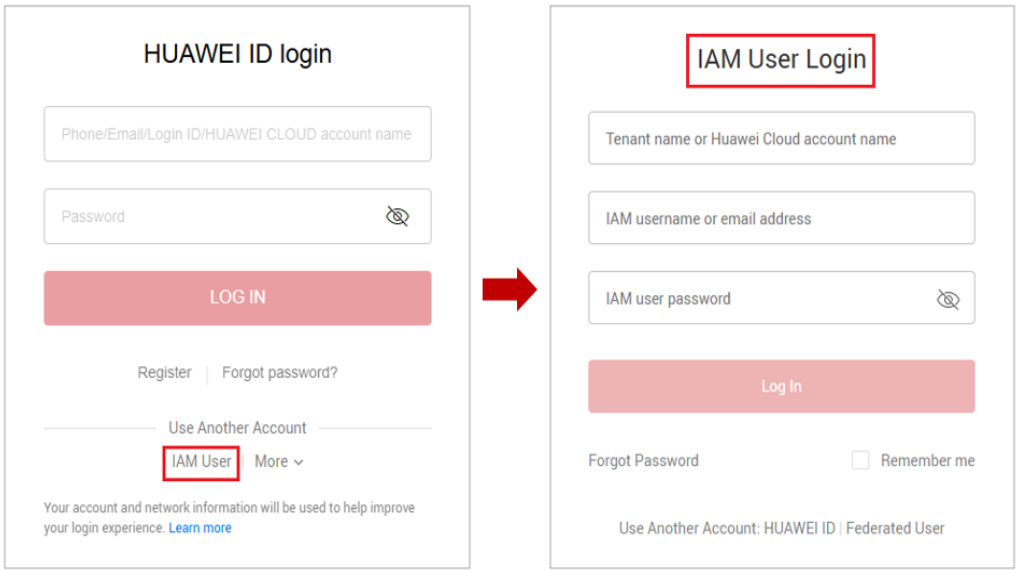
Figure 2-9 Account and IAM users



To log in as an IAM user, do as follows:

Step 1 Click **IAM User** on the login page, and then enter your account name, IAM username or email address, and password.

Figure 2-10 Logging in as an IAM user



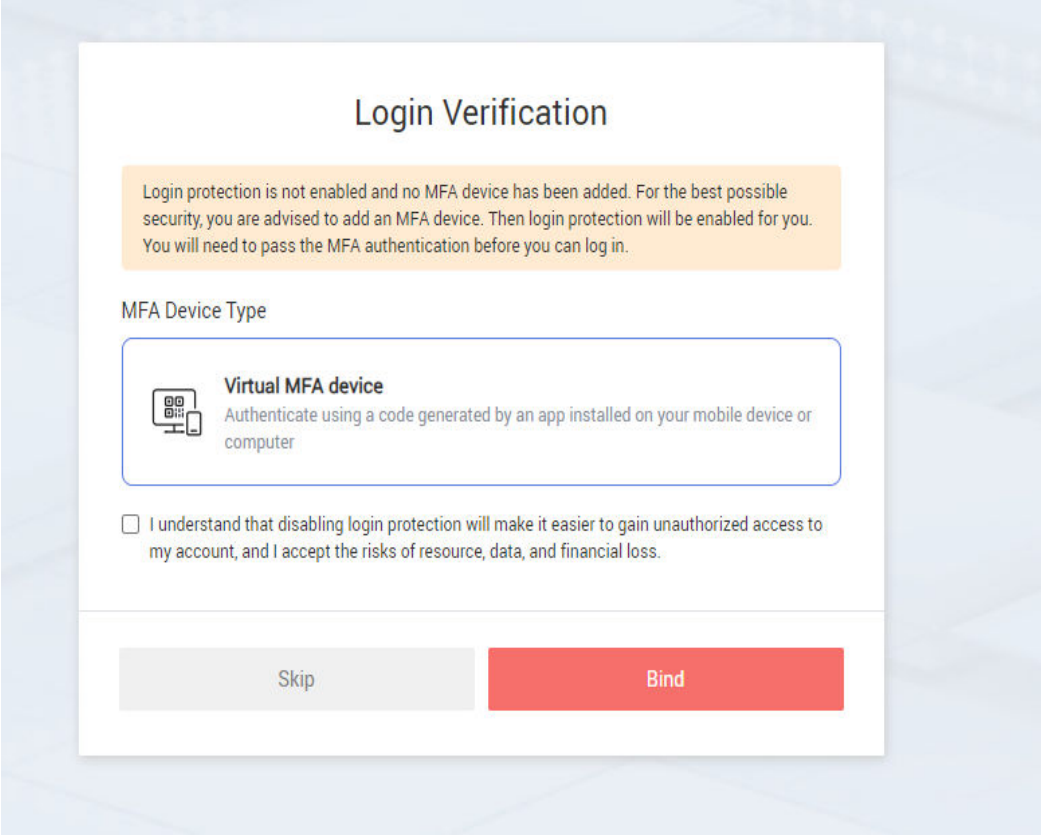
- **Tenant name or Huawei Cloud account name**: The name of the account that was used to create the IAM user. You can obtain the account name from the **administrator**.
- **IAM username or email address**: The username or email address of the **IAM user**. You can obtain the username and password from the **administrator**.
- **IAM user password**: The password of the IAM user (not the password of the account).

Step 2 Click **Log In**.

Step 3 Verify the login.

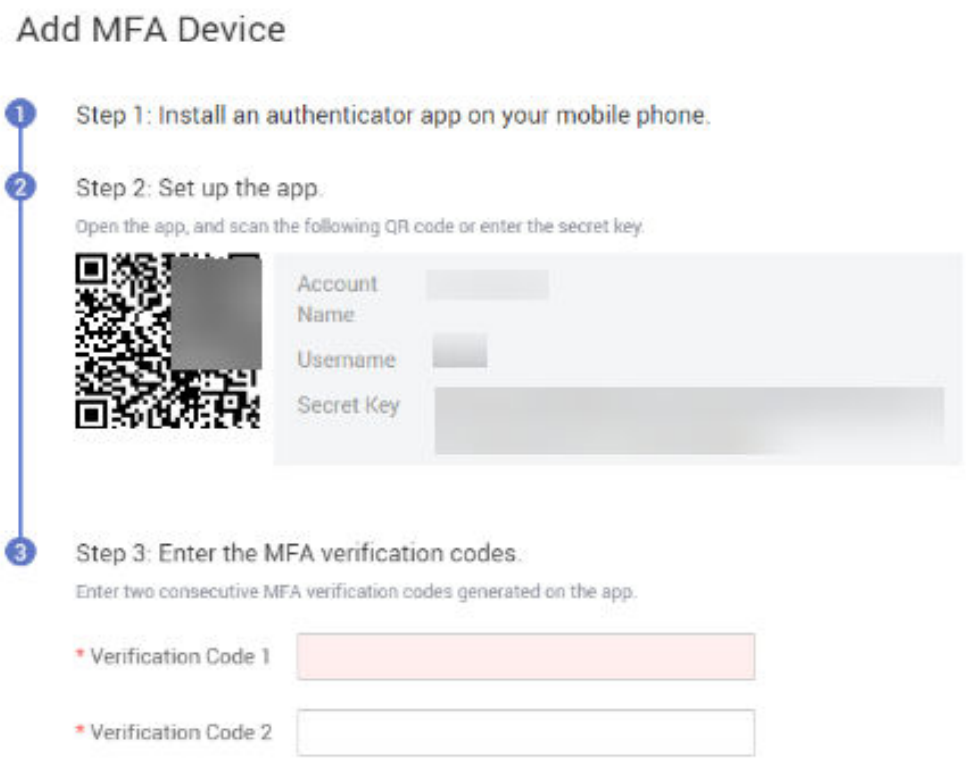
1. If login protection is not enabled for an IAM user or no MFA device is added, you will be directed to a login verification page that suggests binding an MFA device. If you prefer not to bind it, click the confirmation checkbox and click **Skip** to directly access the Huawei Cloud management console.
   - **Binding a virtual MFA device**
     i. On the login verification page, click **Bind**.

Figure 2-11 Login verification



ii. On the **Add MFA Device** page, enter the device name and type, then click **Next** to add a user to your MFA application.

Figure 2-12 Adding an MFA device



Add an MFA device by scanning the QR code or entering the secret key. The Huawei Cloud App is used as an example to describe how to add a user in an MFA application.

- Scanning the QR code

  Open the MFA application and scan the QR code displayed on the **Bind Virtual MFA Device** page. Then the user is added to the MFA application.

- Entering the secret key

  Open the MFA application on your mobile phone, and enter the secret key.

  NOTE

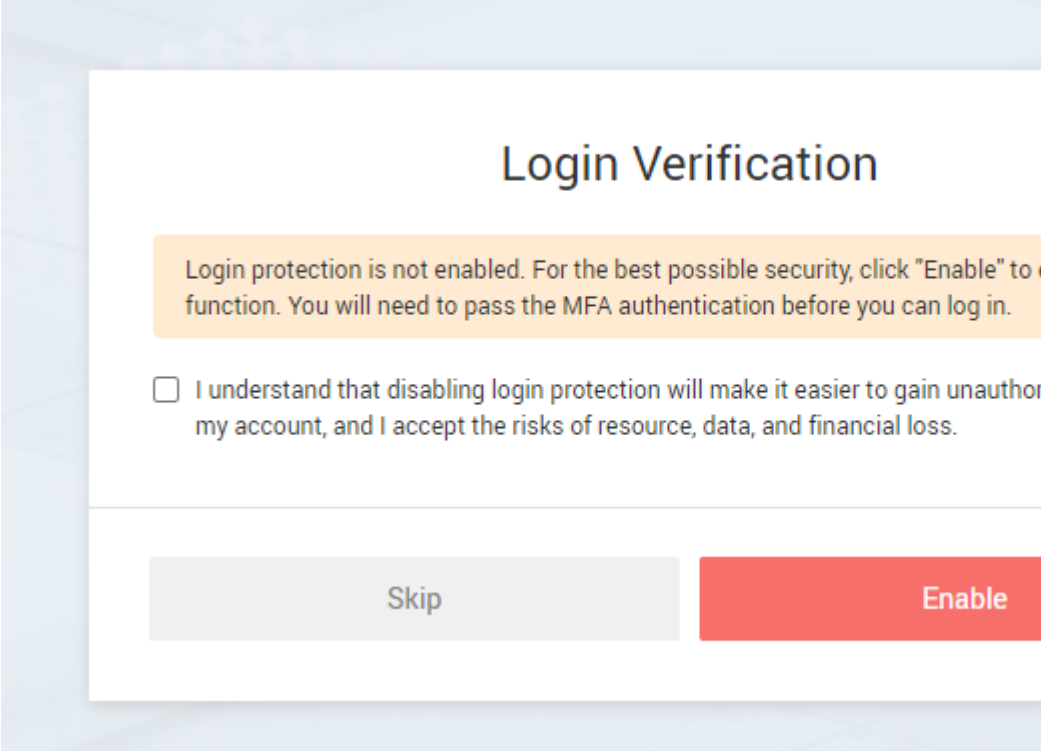
  The user can be manually added only using time-based one-time passwords (TOTP). You are advised to enable automatic time setting on your mobile device.

iii. After a user is added, go to the MFA application to view the verification codes. The code is automatically updated every 30 seconds.

iv. On the **Bind Virtual MFA Device** page, enter two consecutive verification codes and click **OK**. After a virtual MFA device is bound to your account, you can access the Huawei Cloud management console.

2. If login protection is not enabled for an IAM user and an MFA device has been added, you will be directed to a verification page that suggests enabling login protection. If you prefer not to enable it, select the confirmation checkbox and click **Skip** to access the Huawei Cloud management console.
   - **Enabling login protection**
     i. On the login verification page, click **Enable** to enter the MFA authentication page.

     Figure 2-13 Login verification

     ii. Enter the virtual MFA dynamic code, then click **OK** to access the Huawei Cloud management console.

----End

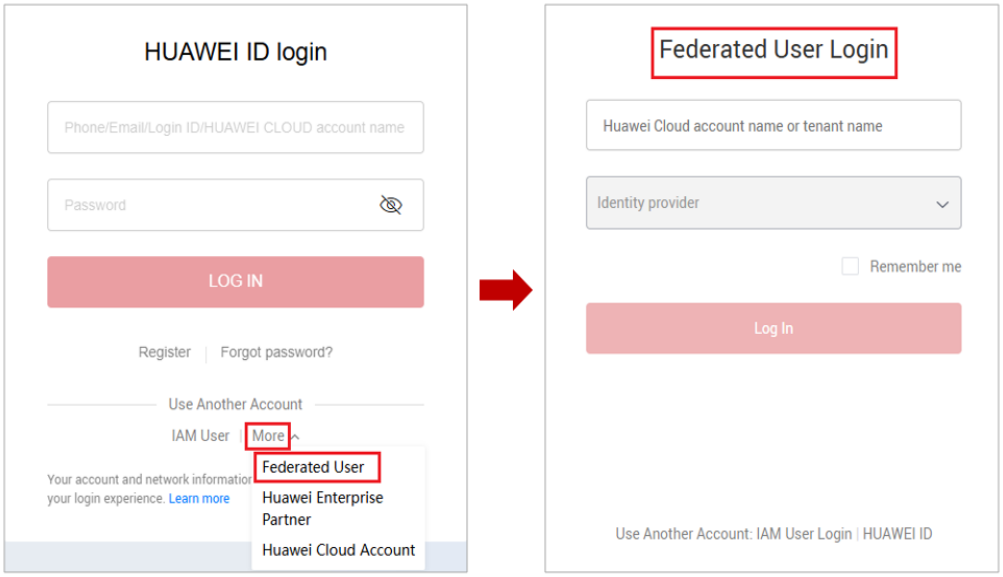
Logging In as a Federated User

Federated users are created in an enterprise management system. After the account administrator **creates an IdP entity** on the IAM console, federated users can log in to Huawei Cloud and use cloud services based on assigned permissions. For details, see **Overview**.

You can log in to Huawei Cloud as a federated user if you have obtained the name of your IdP, the Huawei Cloud account used to create IdP, and the username and password for logging in to your enterprise management system.

Step 1 On the Huawei Cloud login page, click **Federated User**, enter the account name, and select an identity provider.

Figure 2-14 Logging in as a federated user



- **Huawei Cloud account name or tenant name**: The name of the Huawei Cloud account which is used to create the identity provider. You can obtain the account name from the **administrator**.
- **Identity provider**: The name of the identity provider created by the **administrator**. You can obtain the identity provider name from the **administrator**.

Step 2 Click **Log In**. The login page of the enterprise management system is displayed.

Step 3 Enter your username and password for accessing the enterprise management system.

Step 4 Click **Log In**.

----End

3 IAM User Management

3.1 Overview

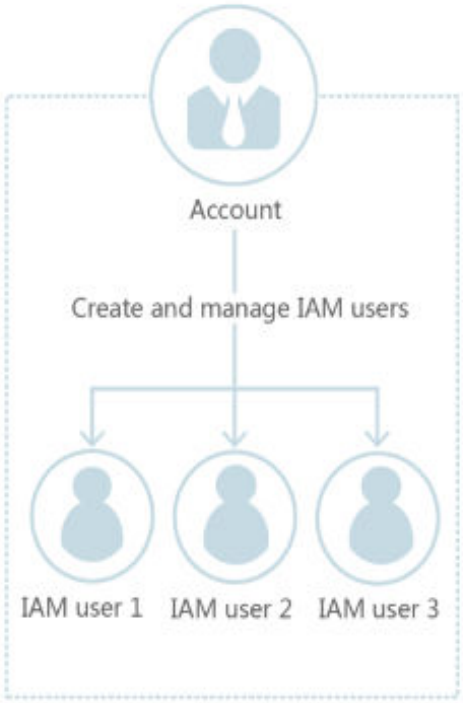
IAM Users

You can use your account to create IAM users and grant them permissions for specific resources. Each IAM user has their own identity credentials (password and access keys) and uses cloud resources based on the granted permissions. IAM users do not own resources.

IAM Users and Accounts

An account and its IAM users have a parent-child relationship. The account owns the resources and makes payments for the resources used by IAM users. It has full access permissions for these resources. IAM users are created by an account, and they only have the permissions granted by the account. The account can modify or revoke the IAM users' permissions at any time. Resources used by IAM users in your account are billed to your account. IAM users do not need to make payments themselves.

Figure 3-1 Relationship between an account and its IAM users



Identifying IAM Users

When you create an IAM user, IAM provides the following methods to identify that user:

- An IAM username, which is specified when you create the IAM user.
- A unique IAM user ID, which is generated when you create the IAM user.

IAM User Credentials and Access Methods

You can access Huawei Cloud in different ways, depending on the credentials of IAM users:

- Console password: IAM users can log in to Huawei Cloud using their passwords. For details, see **Logging In to Huawei Cloud as an IAM User**. If you do not set a console password when creating an IAM user, the user cannot log in using this credential.
- Access keys: You can create access keys for IAM users so that they can make programmatic calls to Huawei Cloud.

3.2 Creating an IAM User

If you are an **administrator** and have purchased multiple resources on Huawei Cloud, such as Elastic Cloud Servers (ECSs), Elastic Volume Service (EVS) disks, and Bare Metal Servers (BMSs), you can create IAM users and grant them permissions required to perform operations on specific resources. This way, you do not need to share the password of your account.

New IAM users do not have any permissions assigned by default. You can assign permissions to new users, or add them to one or more groups and grant permissions to these groups by referring to **Assigning Permissions to a User Group** so that the users can inherit the permissions of the groups. The users then can perform specific operations on cloud services as specified by the permissions.

The default user group **admin** has all permissions required to use all of the cloud resources. Users in this group can perform operations on all the resources, including but not limited to creating user groups and users, modifying permissions, and managing resources.

NOTE

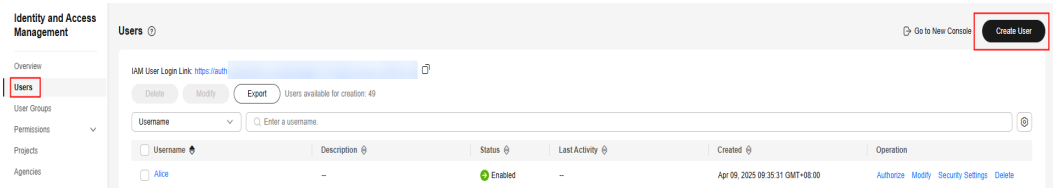
If you delete a user and then create a new user with the same name, you need to grant the required permissions to the new user again.

Procedure

Step 1 Log in to the **IAM console** as the administrator.

Step 2 Choose **Users** from the left navigation pane and click **Create User** in the upper right corner.

Figure 3-2 Creating an IAM user



Step 3 Specify the user details on the **Create User** page. To create more users, click **Add User**. You can add a maximum of 10 users at a time.

Figure 3-3 Specifying user details

Table 3-1 User details

Parameter	Description
Username	The name is user-defined and must be different from that of any other account or any IAM user in the account.
Email Address	The email address is user-defined and must be different from that of any other account or any IAM user in the account. It can be used to authenticate the IAM user and reset the password.

Parameter	Description
Mobile Number	The mobile number is user-defined and must be different from that of any other account or any IAM user in the account. It can be used to authenticate the IAM user and reset the password.
External Identity ID	Identity of an enterprise user in IAM user SSO. This parameter must be specified if you want to configure **virtual user SSO via SAML** for an IAM user. The value contains a maximum of 128 characters.

NOTE

- IAM users can log in to Huawei Cloud using the username, email address, or mobile number.
- If users forget their passwords, they can reset the passwords through email address or mobile number verification. If no email addresses or mobile numbers have been associated with users, users need to request the administrator to reset their passwords.

Step 4 Specify **Access Type**.

Figure 3-4 Selecting access types

Table 3-2 Access types

Access Type	Description
Programmatic access	An access key or password is generated for the IAM user. This type allows access to cloud services using development tools, such as APIs, CLI, and SDKs.
Management console access	A password is generated for the IAM user. This type allows access to cloud services using the management console. A password is mandatory for login.

NOTE

- If the user accesses cloud services only by using the management console, select **Management console access** for **Access Type** and **Password** for **Credential Type**.
- If the user accesses cloud services only through programmatic access, select **Programmatic access** for **Access Type** and **Access key** for **Credential Type**
- If the user needs to use a password as the credential for programmatic access to certain APIs, select **Programmatic access** for **Access Type** and **Password** for **Credential Type**.
- If the user needs to perform access key verification when using certain services on the console, select **Programmatic access** and **Management console access** for **Access Type**, and select **Access key** and **Password** for **Credential Type**. For example, the user needs to perform access key verification before creating a data migration job on the Cloud Data Migration (CDM) console.

Step 5 Specify **Credential Type**.

Figure 3-5 Selecting credential types

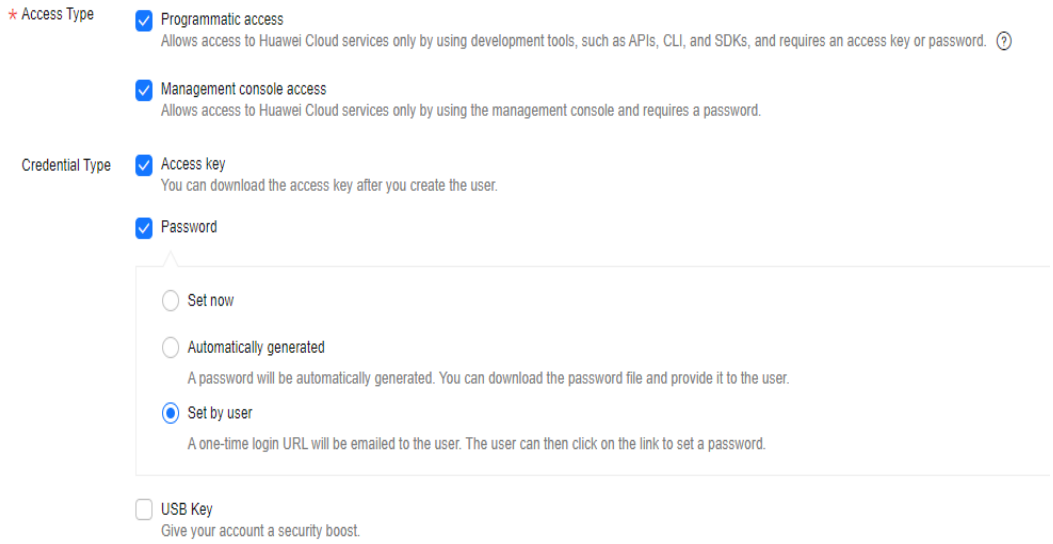


Table 3-3 Credential types

Credential Type		Description
Access key		After creating the user, you can download the **access key (AK/SK)** generated for the user. **Each user can have a maximum of two access keys.**
Password	Set now	Set a password for the user and determine whether to require the user to reset the password at the first login. If you will use the IAM user by yourself, you are advised to select this option, enter a password, and deselect **Require password reset at first login**.

Credential Type		Description
	Automatically generated	The system automatically generates a login password for the user. After the user is created, you can download the EXCEL password file and provide the password to the user. The user can then use this password for login. The password file must be downloaded upon the user creation. If you cancel the download, the password file cannot be obtained again. You can reset the user password by referring to **Modifying Security Settings for an IAM User**. This option is available only when you create an individual user.
	Set by user	A one-time login URL will be emailed to the user. The user can click the link to log in to the console and set a password. If you do not use the IAM user by yourself, select this option and enter the email address and mobile number of the IAM user. The user can then set a password by clicking the one-time login URL sent over email. The login URL is valid for **seven days**.
USB Key		A USB key is a device that stores user credentials. You can use a USB key, rather than a password to verify your identity. This option is more secure, as there is no password to be leaked. If this option is selected, the IAM user can only use the USB key to log in. The IAM user cannot use the password or change the login mode.

Table 3-4 Recommended configurations

Management Console Access	Programmatic Access	Credential Type	Recommended Access Type	Recommended Credential Type
Select	Deselect	There are no special requirements.	Management console access	Password
Deselect	Select	There are no special requirements.	Programmatic access	Access key
Deselect	Select	A password is required as a credential for programmatic access (required by some APIs).	Programmatic access	Password

Management Console Access	Programmatic Access	Credential Type	Recommended Access Type	Recommended Credential Type
Select	Select	The access key (entered by the IAM user) needs to be verified on the console. For example, the user needs to perform access key verification before creating a data migration job in the Cloud Data Migration (CDM) console.	Programmatic access and management console access	Password and access key

Step 6 Enable or disable login protection. This option is available only when you have selected **Management console access** for **Access Type**.

Figure 3-6 Login protection enabled

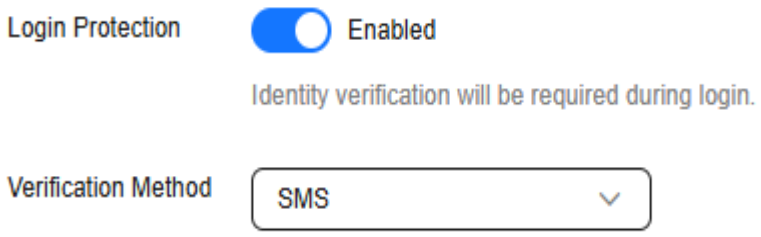
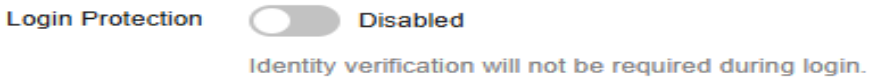


Figure 3-7 Login protection disabled



- Log in protection enabled (Recommend):Log in protection enabled: The user needs to enter a verification code in addition to the username and password for login.

  You can choose from SMS-, email-, and virtual MFA–based login verification.
- Login protection disabled: To enable login protection after the user is created, see **Login Protection**.

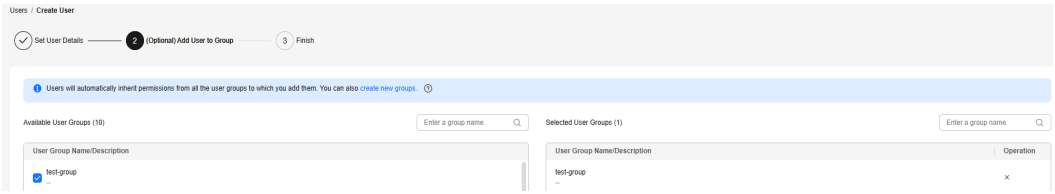
Step 7 Enable or disable API login protection. This function is available when only login protection is enabled and the verification mode is set to virtual MFA.

1. API login protection enabled: Both a password and a virtual MFA device are required to obtain an IAM user token. To obtain an IAM user token, see **Obtaining a User Token Through Password and Virtual MFA Authentication**.

2. API login protection disabled: You can enable API login protection after user creation. Locate the target user, and click **Security Settings** in the **Operation** column. In the displayed tab, click next to **Verification Method** of the **Login Protection** function, enable this function, and select **Virtual MFA device**.

Step 8 Click **Next**. You can optionally select user groups for the user. Once the user is added to user groups, the user will inherit permissions assigned to the groups.

Figure 3-8 Adding the user to a user group



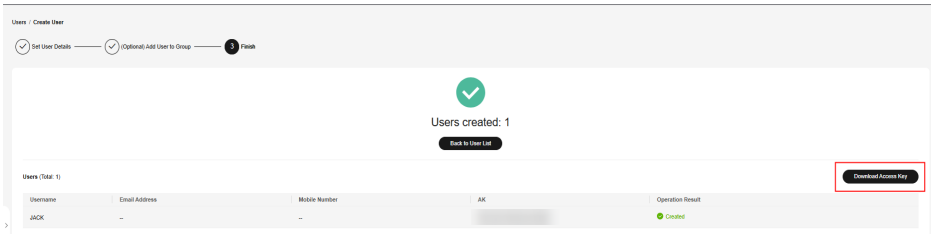
NOTE

- You can also create a new group and add the user to that group.
- If you want the user to be an administrator, add the user to the default group **admin**.
- You can add a user to a maximum of 10 user groups.

Step 9 Click **Create**. The IAM user will be displayed in the user list.

- If you have selected **Access key** for **Credential Type** in **Step 5**, you can download the access key on the **Finish** page.
- If you have selected **Password** > **Automatically generated** for **Credential Type** in **Step 5**, you can download the password file on the **Finish** page.

Figure 3-9 Users created successfully



----End

Related Operations

- IAM users created without being added to any groups do not have any permissions. The administrator can assign permissions to these IAM users on the IAM console. IAM users can also assign permissions to themselves. Then the users can use cloud resources based on the assigned permissions. For details, see **Assigning Permissions to an IAM User**.
- Accounts and IAM users use different methods to log in. For details about IAM user login, see **Logging In to Huawei Cloud as an IAM User**.

3.3 Assigning Permissions to an IAM User

IAM users created without being added to any groups do not have any permissions. The administrator can assign permissions to these IAM users on the IAM console. IAM users can also assign permissions to themselves. After authorization, the users can use cloud resources in your account as specified by their permissions.

Constraints

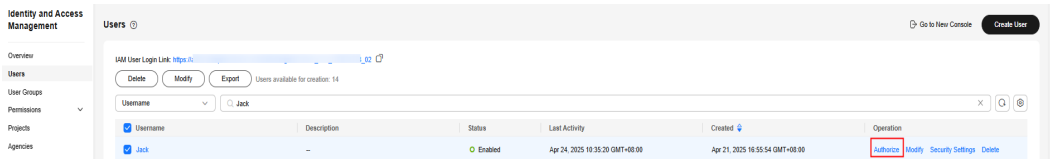
A maximum of 500 permissions (including system-defined permissions and custom policies) can be assigned to each IAM user for enterprise projects.

Procedure

Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user list, click **Authorize** in the row that contains the target user.

Figure 3-10 Authorizing an IAM user

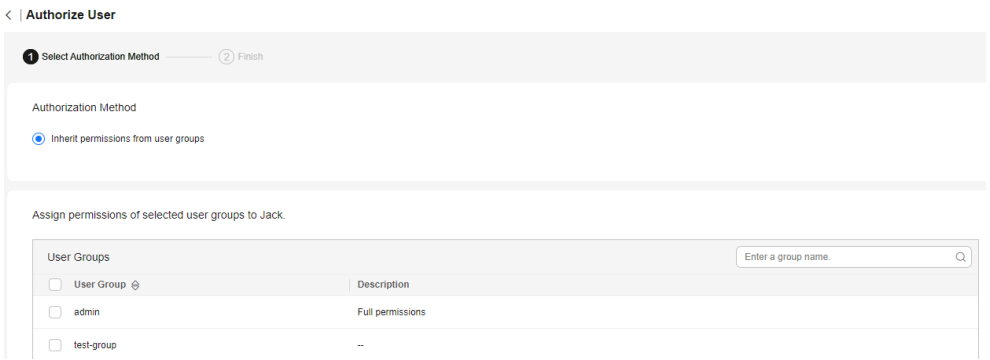


Step 3 On the **Authorize User** page, select an authorization mode and permissions.

- **Inherit permissions from user groups**: Add the IAM user to certain groups to inherit their permissions.

  If you select this option, select the user groups which the user will belong to.

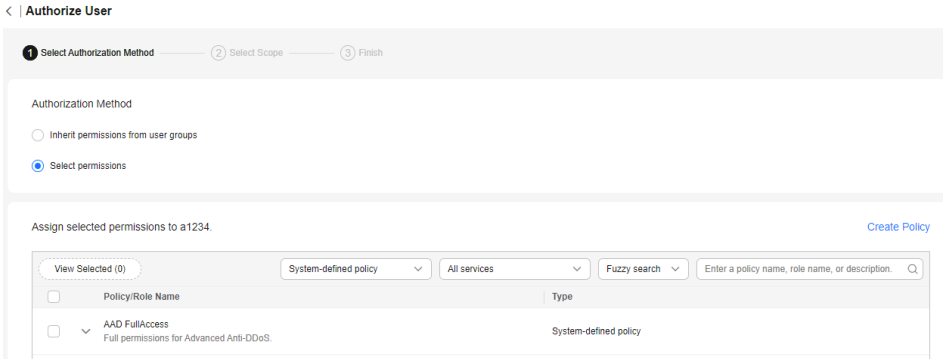
  Figure 3-11 Enterprise Project function not enabled

- **Select permissions**: Directly assign specific permissions to the IAM user. You can assign permissions directly to IAM users only when Enterprise Project is enabled. To enable Enterprise Project, see **Enabling the Enterprise Project Function**.

  If you select this option, select permissions, click **Next** in the lower right, and then go to step **Step 4**.

Figure 3-12 Enterprise project function enabled



NOTE

- If you add an IAM user to the default group **admin**, the user becomes an administrator and can perform all operations on all cloud services.
- If a user is added to multiple user groups, the user inherits the permissions assigned to all these groups.
- For details on the system-defined permissions of all cloud services supported by IAM, see **System-defined Permissions**.
- If you have enabled enterprise management, you cannot create subprojects in IAM.

Step 4 On the **Select Scope** page, select enterprise projects that the IAM user can access. You do not need to perform this step if you have selected **Inherit permissions from user groups**.

Step 5 Click **OK**.

You can go to the **Permissions** > **Authorization** page and view or modify the permissions of the IAM user.

NOTE

In the enterprise project authorization, if OBS permissions are assigned, they will be applied about 15 to 30 minutes after the authorization is complete.

----End

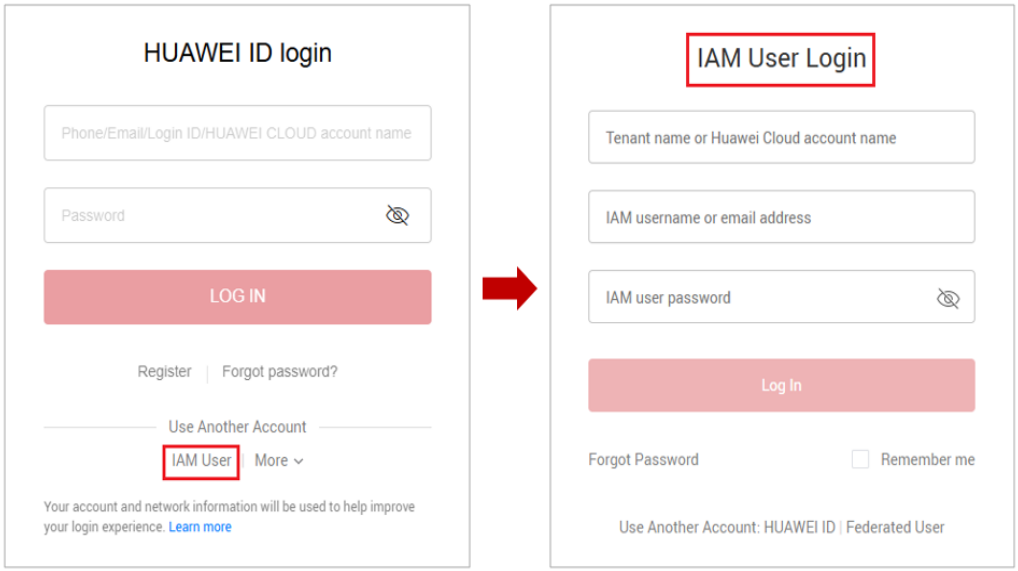
3.4 Logging In to Huawei Cloud as an IAM User

To log in as an IAM user, you can choose **IAM User** on the login page or obtain the IAM user login link from the administrator.

Method 1: Logging In by Clicking IAM User on the HUAWEI ID Login Page

Step 1 Click **IAM User** on the login page, and then enter your account name, IAM username or email address, and password.

Figure 3-13 Logging in as an IAM user



- **Tenant name or Huawei Cloud account name**: The name of the account that was used to create the IAM user. You can obtain the account name from the **administrator**.
- **IAM username or email address**: The username or email address of the **IAM user**. You can obtain the username and password from the **administrator**.
- **IAM user password**: The password of the IAM user (not the password of the account).

Step 2 Click **Log In**.

NOTE

- If the IAM user has not been added to any groups, you do not have permissions to access any cloud services. In this case, contact the administrator and request permissions needed. For details, see **Creating a User Group and Assigning Permissions** and **Adding IAM Users to or Removing IAM Users from a User Group**.
- If the IAM user has been added to the default group **admin**, the user has administrator permissions and can perform all operations on all cloud services.

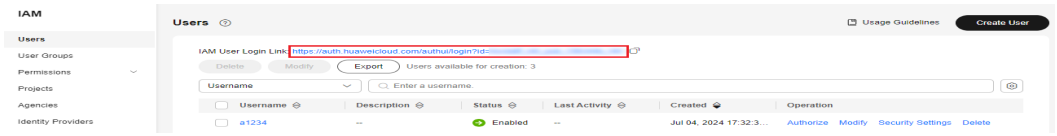
----End

Method : Logging In Using the IAM User Login Link

You can obtain the IAM user login link from the administrator and then log in using this link. When you visit the link, the system displays the login page and automatically populates the account name. You only need to enter your username and password.

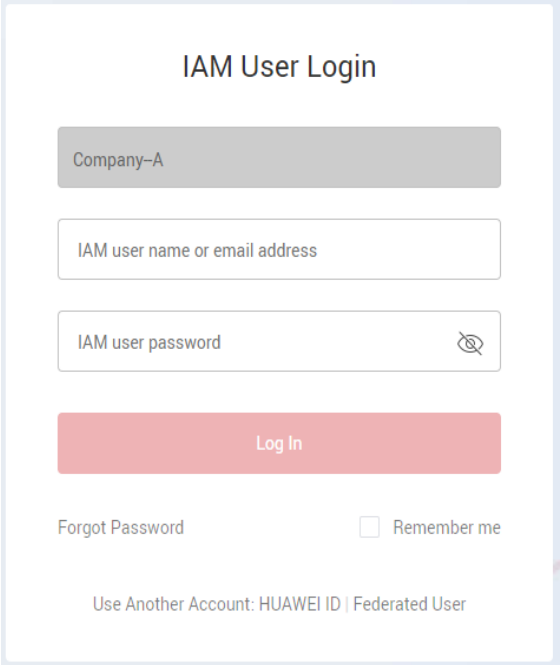
Step 1 Obtain the IAM user login link from the administrator, who can copy the login link from the **IAM console**.

Figure 3-14 IAM user login link



Step 2 Paste the link in the address bar of a browser, press **Enter**, and enter the IAM username/email address and password, and click **Log In**.

Figure 3-15 Logging in using the IAM user login link



----End

3.5 Managing IAM User Information

As an administrator, you can view the basic information about an IAM user on its details page, including its status, ID, access type, creation time, external identity ID, and description. Only the basic information about an IAM user can be modified. The account information cannot be modified. The username, user ID, and creation time can be viewed but cannot be modified.

Viewing Basic Information About an IAM User

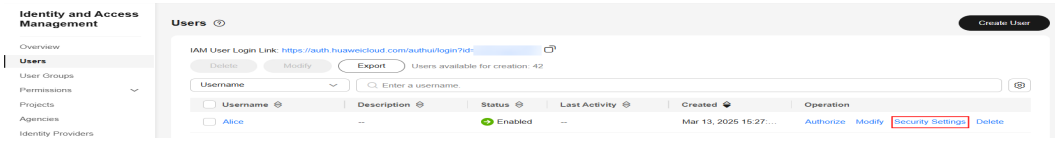
Step 1 Log in to the **IAM console** as the administrator.

Step 2 Click  on the right of the search box to customize the columns displayed on the list. The **Username**, **Status**, and **Operation** columns are displayed by default. You can also select **Description**, **Last Activity**, **Created**, **Access Type**, **Login Authentication**, **Virtual MFA Status**, **Password Age**, **Access Key (Status, Age, and AK)**, and **External Identity ID**.

The **Last Activity** column only displays your first login time if you log in as an account or IAM user more than once in a 5-minute span. If you just use the account to obtain a token, rather than logging in, the last activity time would still be updated.

Step 3 In the user list, click a username or click **Security Settings** in the **Operation** column to access the user details page.

Figure 3-16 Going to the IAM user security settings page



Step 4 View the basic information about the IAM user.

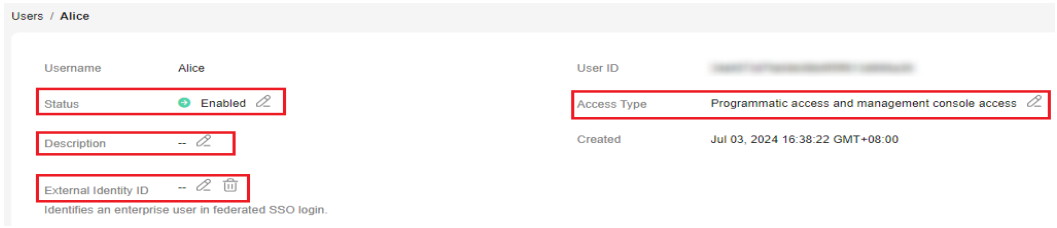
----End

Modifying Basic Information About an Individual IAM User

Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user list, click a username or click **Security Settings** in the **Operation** column to access the user details page.

Figure 3-17 Modifying the status, access type, description, and external identity ID of an IAM user



Step 3 Modify the basic information about an IAM user on its details page as an administrator.

- **Status**: New IAM users are enabled by default. You can set **Status** to **Disabled** to disable an IAM user. A disabled user is no longer able to log in to Huawei Cloud through the management console or programmatic access. IAM users can also modify their statuses.
- **Access Type**: You can change the access type of the IAM user.

NOTE

- Pay attention to the following when you set the access type of an IAM user:
  - If the user accesses cloud services only by using the management console, select **Management console access** for **Access Type** and **Password** for **Credential Type**.
  - If the user accesses cloud services only through programmatic calls, select **Programmatic access** for **Access Type** and **Access key** for **Credential Type**.
  - If the user needs to use a password as the credential for programmatic access to certain APIs, select **Programmatic access** for **Access Type** and **Password** for **Credential Type**.
  - If the user needs to perform access key verification when using certain services in the console, such as creating a data migration job in the Cloud Data Migration (CDM) console, select **Programmatic access** and **Management console access** for **Access Type**, and select **Access Key** and **Password** for **Credential Type**.
- If the access type of the user is **Programmatic access** or both **Programmatic access** and **Management console access**, deselecting **Programmatic access** will restrict the user's access to cloud services. Exercise caution when performing this operation.

- **Description**: You can modify the description of the IAM user.
- **External Identity ID**: Identifies an enterprise user in federated login using SSO.

----End

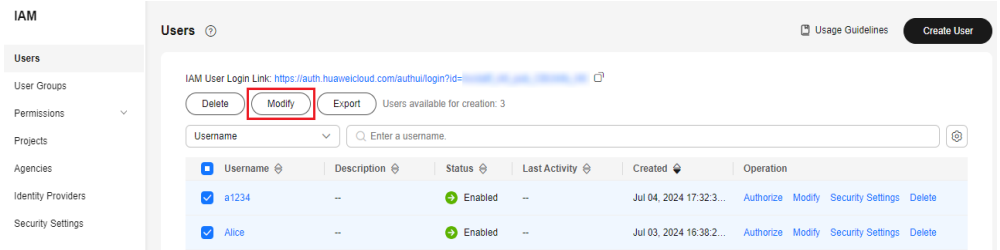
Batch Modifying IAM User Information

IAM allows you to batch modify the status, access type, verification method, login password, mobile number, and email address of IAM users. The following describes how to batch modify the status of IAM users. The methods of modifying other information about users are similar to this method.

Step 1 Log in to the **IAM console**. In the navigation pane, choose **Users**.

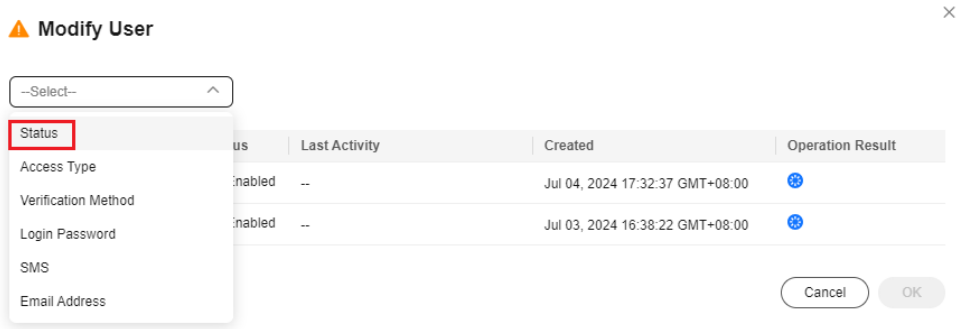
Step 2 In the user list, select the users whose information you want to modify, and click **Modify** above the user list.

Figure 3-18 Modifying user information



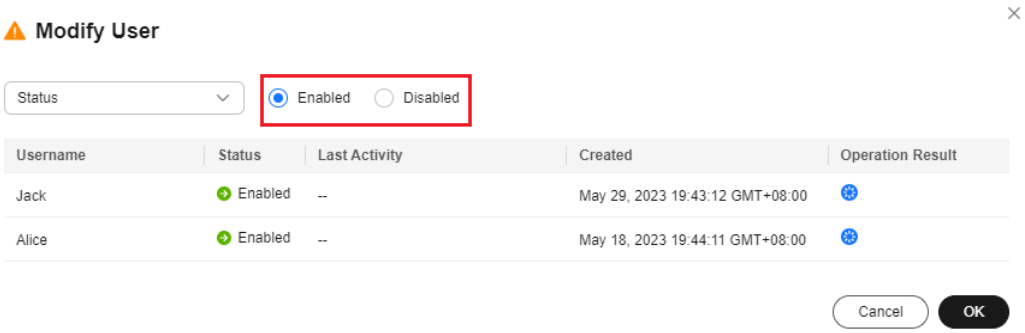
Step 3 Select the property you want to modify. In this example, select **Status** from the drop-down list.

Figure 3-19 Selecting the status property



Step 4 Select the target status to be configured for the selected IAM users.

Figure 3-20 Selecting the target status



NOTE

Make sure that this user is no longer in use. Disabling an active user may affect services.

Step 5 Click **OK**.

Step 6 In the displayed dialog box, click **OK** to confirm the change.

----End

3.6 Modifying the User Group Which an IAM User Belongs to

An IAM user inherits permissions from the user groups that the user belongs to. You can change the permissions assigned to an IAM user by changing the user groups that the user belongs to.

Constraints

Your account belongs to the default group **admin**, which cannot be changed.

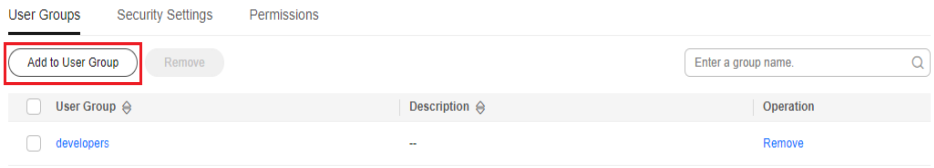
Procedure

Step 1 Log in to the **IAM console** as the administrator.

Step 2 Click a username to go to the user details page.

Step 3 Click **Add to User Group** on the **User Groups** tab.

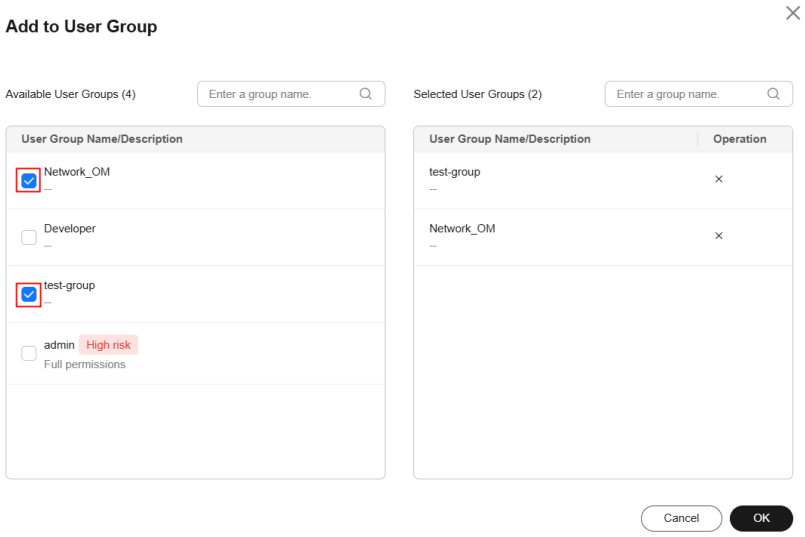
Figure 3-21 Adding a user to a user group



Step 4 In the **Add to User Group** dialog box, select the target user groups which you want to add the user to.

A user can be added to one or more user groups.

Figure 3-22 Configuring group membership

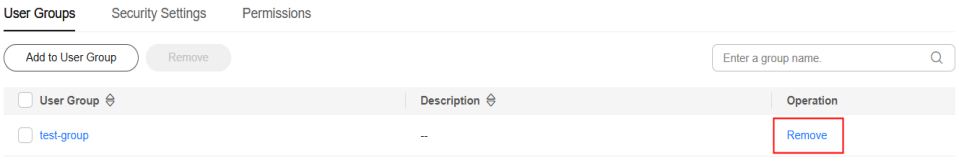


Step 5 Click **OK**. The selected user groups will be displayed in the user group list.

After a user is added to a user group, the user inherits all the permissions of it.

Step 6 To remove an IAM user from a user group, locate the target group and click **Remove** in the **Operation** column. In the displayed dialog box, click **OK**. After the user is removed from a group, the permissions inherited from the group will be revoked.

Figure 3-23 Removing a user from a user group



----End

Related Operations

To modify the permissions of a user group, see **Managing Permissions of a User Group**.

3.7 Managing Access Keys for an IAM User

An access key consists of an access key ID (AK) and secret access key (SK) pair. You can use an access key to access Huawei Cloud using development tools, including APIs, CLI, and SDKs. Access keys cannot be used to log in to the console. AK is a unique identifier used in conjunction with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.

As an administrator, you can manage access keys for IAM users who have forgotten their access keys and do not have access to the console.

Constraints

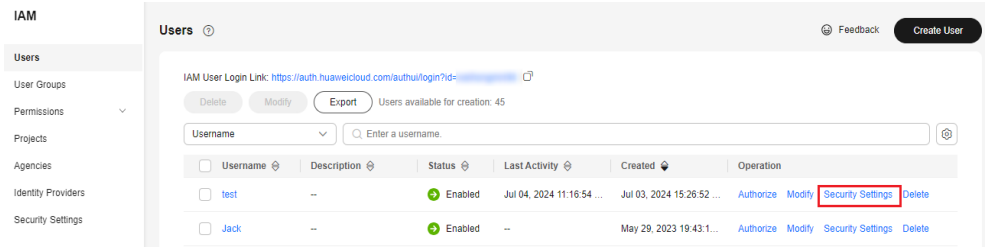
- Federated users can only create temporary access credentials (temporary AKs/SKs and security tokens). For details, see **Temporary Access Key (for Federated Users)**.
- If a user is authorized to use the console, the user can **manage access keys** on the **My Credentials** page.
- Access keys are identity credentials used to call APIs. The account administrator and IAM users can only use their own access keys to call APIs.
- If an access key is used more than once in a 15-minute span, the **Last Used** column in the **Access Keys** area only displays the first use time.
- Each IAM user has a maximum of two access keys, which are permanently valid. For security purposes, change the access keys of IAM users periodically.
- If you did not download an access key when creating it, you cannot obtain its SK after closing the dialog box. In this case, you can delete the current access key and create a new one.
- Once deleted, an IAM user's access key cannot be recovered. Ensure that the deletion will not affect services.

Creating Access Keys for an IAM User

Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user list, click a username or click **Security Settings** in the **Operation** column to access the user details page.

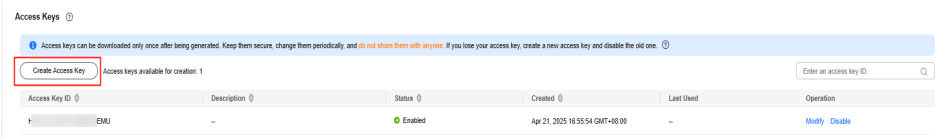
Figure 3-24 Managing access keys for an IAM user



Step 3 Click the **Security Settings** tab. Click **Create Access Key** in the **Access Keys** area.

If operation protection is enabled, you (the administrator) need to enter a verification code or password for identity authentication when creating an access key.

Figure 3-25 Creating an access key



Step 4 Click **OK**. An access key is automatically generated. Download the access key and provide it to the IAM user.

If you did not download an access key when creating it, you cannot obtain its SK after closing the dialog box. In this case, you can delete the current access key and create a new one.

----End

Deleting Access Keys for an IAM User

Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user list, click a username or click **Security Settings** in the **Operation** column to access the user details page.

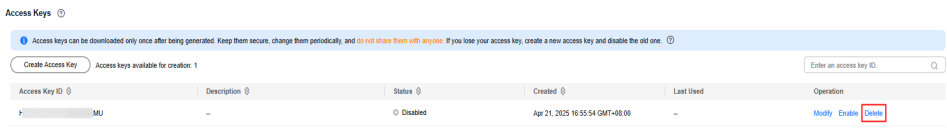
Step 3 Click the **Security Settings** tab. In the **Access Keys** area, locate the target access key and click **Disable** in the **Operation** column.

Step 4 In the displayed dialog box, click **OK**.

Step 5 Click **Delete** in the **Operation** column of the disabled access key. Ensure that the deletion will not affect your services.

If operation protection is enabled, you (the administrator) need to enter a verification code or password for identity authentication when deleting an access key.

Figure 3-26 Deleting an access key



Step 6 Click **OK**.

----End

Enabling or Disabling an Access Key

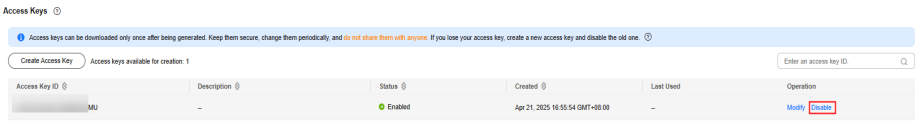
Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user list, click a username or click **Security Settings** in the **Operation** column to access the user details page.

Step 3 Click the **Security Settings** tab. In the **Access Keys** area, locate the access key to be disabled and click **Disable** in the **Operation** column.

If operation protection is enabled, you (the administrator) need to enter a verification code or password for identity authentication when disabling an access key.

Figure 3-27 Disabling an access key



Step 4 In the displayed dialog box, click **OK** to disable the access key.

The method of enabling an access key is similar to that of disabling an access key.

----End

3.8 Modifying Security Settings for an IAM User

As an administrator, you can modify the password, MFA device, login protection, and access keys of an IAM user.

Constraints

- If the password of an IAM user is automatically generated, it cannot be changed on the **Security Settings** tab of the IAM console. To change the password, go to the **Basic Information** page of My Account.
- IAM users can change their passwords on the **Basic Information** tab. If you want to change the password of your account, see **How Do I Change My Password?**
- By default, only the IAM user's MFA device can be changed on the **Security Settings** tab. The MFA device of the account cannot be changed. To change the MFA device of the account, grant the permissions needed to add and unbind the MFA device.
- The mobile number and email address of the IAM user cannot be the same as those of the account or other IAM users.

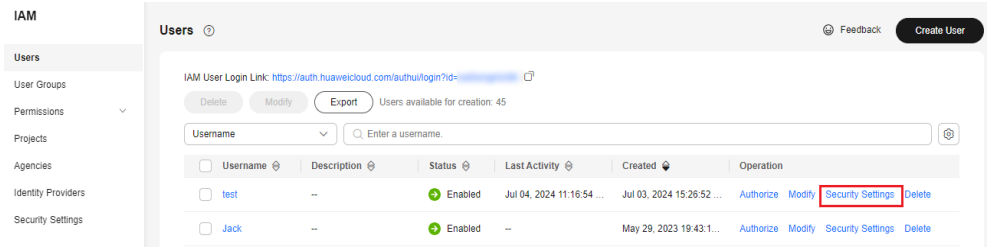
Changing the Password of an IAM User

As an administrator, you can reset the password of an IAM user if the user has forgotten the password and no email address or mobile number has been bound to the user. You can also delete the login password of the user. This will disable their access to Huawei Cloud. Exercise caution when performing this operation.

Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user list, click a username or click **Security Settings** in the **Operation** column to access the user details page.

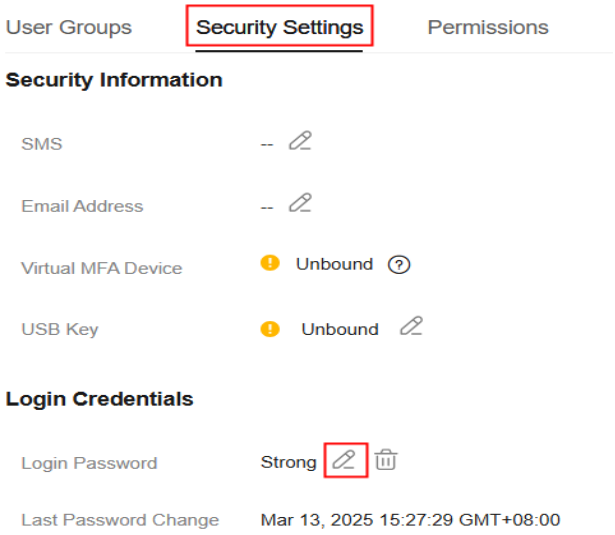
Figure 3-28 Changing the password of an IAM user



Step 3 Click the **Security Settings** tab. In the **Login Credentials** area, click in the **Login Password** row to reset the login password for the IAM user.

- **Set by user**: A one-time login URL will be emailed to the user. The user can then click the link to set a password.
- **Automatically generated**: A password will be automatically generated and then sent to the user by email.
- **Set now**: You set a new password and send the new password to the user.

Figure 3-29 Changing a password



----End

Changing the MFA Device for an IAM User

You can only change the MFA device for an IAM user, but not for the account.

Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user list, click a username or click **Security Settings** in the **Operation** column to access the user details page.

Step 3 Click the **Security Settings** tab and change the MFA device of the IAM user.

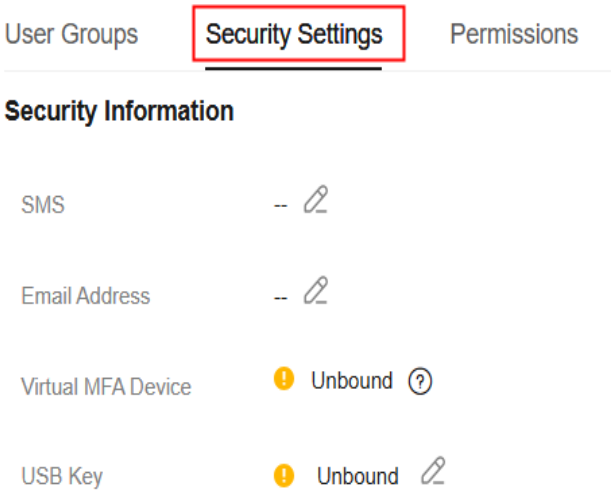
- Change the mobile number or email address of the user. The mobile number and email address of the user can be deleted.

NOTE

The mobile number and email address of the IAM user cannot be the same as those of the account or other IAM users.

- Reset the MFA device for a user. For more information about MFA authentication and virtual MFA device, see **MFA Authentication**.
- Bind a USB key to an IAM user or unbind the USB key from the user.

Figure 3-30 Changing the MFA device



----End

Modifying the Login Protection Configuration for an IAM User

Login protection is disabled by default. If you enable this option, the user will need to enter a verification code in addition to the username and password when logging in to the console.

Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user list, click a username or click **Security Settings** in the **Operation** column to access the user details page.

Step 3 Click the **Security Settings** tab and modify the login protection configuration of the IAM user. This option is disabled by default. You can choose from the following methods for secondary verification:

- SMS
- Email address
- Virtual MFA device

Step 4 Enable or disable (default) API login protection as needed when you select **Virtual MFA device**. API login protection asks you for both a password and a virtual MFA device to obtain an IAM user's security token. Without API login protection, you can obtain the token with only a password. To obtain an IAM user token, see **Obtaining a User Token Through Password and Virtual MFA Authentication**.

----End

Related Operations

- If you are an IAM user and need to change your mobile number, email address, or virtual MFA device, see **Security Settings Overview**.
- To manage access keys of IAM users, see **Managing Access Keys for an IAM User**.

3.9 Managing Permissions Assigned to IAM Users

As an administrator, you can view or delete permissions assigned to IAM users on the **Permissions** tab of the IAM console.

Constraints

- If the principal type of the authorization record is a user group, deleting the permissions will affect all users in the group. To remove the assigned permissions, go to the user group details page. For details, see **Managing Permissions Assigned to IAM Users**.
- Deleting the permissions of an IAM user will also delete the permissions assigned to the group that the user belongs to. All users in the group will no longer have the permissions. Exercise caution when performing this operation.

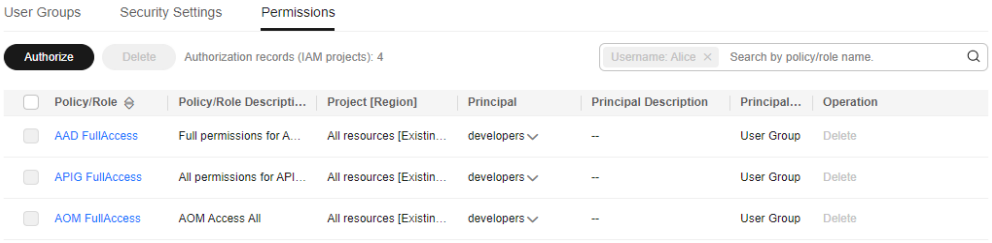
Procedure

Step 1 Log in to the **IAM console** as the administrator.

Step 2 Click a username to go to the user details page.

Step 3 Click the **Permissions** tab to view the permissions assigned to the IAM user.

Figure 3-31 Permissions assigned to an IAM user



----End

Related Operations

To view all authorization records under your account, see **Authorization Records**.

3.10 Deleting IAM Users

You can delete an IAM user that is no longer needed.

Constraints

After an IAM user is deleted, they can no longer log in and their username, password, access keys, and authorizations will be cleared and cannot be recovered.

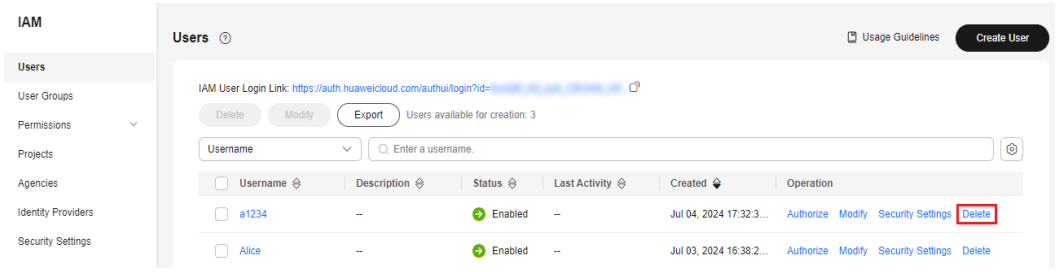
- Make sure that the users to be deleted are no longer needed. If you are not sure, disable them rather than delete them so that they can be enabled if any service failures occur. To disable an individual IAM user, see **Modifying Basic Information About an Individual IAM User**. To disable multiple IAM users at a time, see **Batch Modifying IAM User Information**.
- To remove an IAM user from a user group, see **Adding IAM Users to or Removing IAM Users from a User Group**.

Procedure

Step 1 Log in to the **IAM console**. In the navigation pane, choose **Users**.

Step 2 Click **Delete** in the row containing the IAM user you want to delete, and click **OK**.

Figure 3-32 Deleting an IAM user



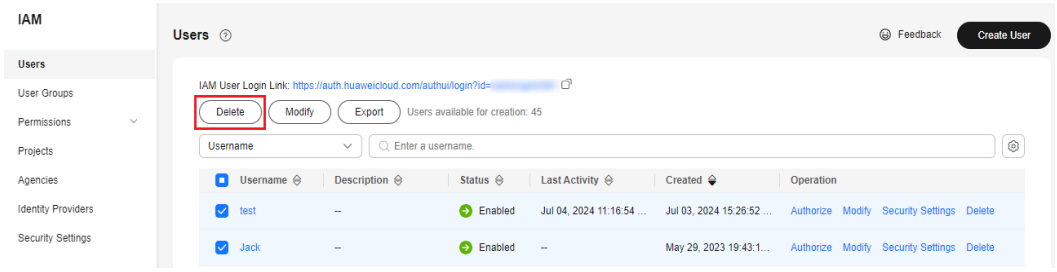
----End

Batch Deleting IAM Users

Step 1 Log in to the **IAM console**. In the navigation pane, choose **Users**.

Step 2 In the user list, select the users to be deleted and click **Delete** above the user list.

Figure 3-33 Batch deleting IAM users



Step 3 In the displayed dialog box, confirm the deletion and click **OK**.

----End

4 User Group Management

4.1 Overview

User Groups

A user group is a collection of IAM users. User groups allow you to assign permissions to users in the groups, making it easier to manage the permissions for those users.

For example, each account has a preset admin user group by default. The admin user group has full permissions for cloud services and resources. Any IAM user in the admin user group automatically has the admin group permissions. If a new user joins your organization and requires the admin permissions, you can grant the permissions by adding the user to the admin user group. If a user changes the job responsibilities and no longer needs the admin permissions, you can simply remove the user from the admin group, instead of changing the user's permissions.

To follow the principal of least privilege (PoLP), you are advised to create user groups and grant only the permissions needed for specific tasks to the user groups, rather than directly adding IAM users to the admin group.

Characteristics of User Groups

- A user group can contain multiple IAM users, and an IAM user can be added to multiple user groups.
- User groups cannot be nested. They can only contain IAM users, not other user groups.
- By default, each account has only one preset admin user group. You need to create different user groups and assign different permissions to the groups.
- The number and size of IAM resources in an account are limited. For example, the number of user groups in an account and the number of IAM users that can be added to a user group are limited. For details, see **Notes and Constraints**.

4.2 Creating a User Group and Assigning Permissions

As an administrator, you can create user groups and grant them permissions using policies or roles. Users added to the user groups inherit permissions from the user groups. IAM users can assign permissions to themselves. IAM provides general permissions (such as administrator or read-only permissions) for each cloud service, which you can assign to user groups. Users in the groups can then use cloud services based on the assigned permissions. For details, see **Assigning Permissions to an IAM User**. To learn about system-defined permissions of all cloud services, see **System-defined Permissions**.

Prerequisites

Before creating a user group, learn about the following:

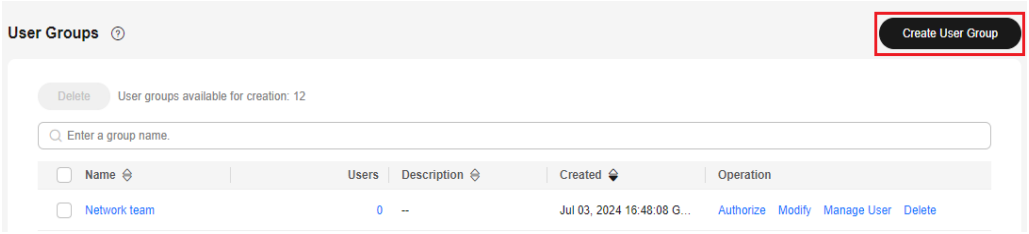
- **Basic concepts** of permissions
- **System-defined permissions** provided by IAM

Creating a User Group

Step 1 Log in to the **IAM console** as the administrator.

Step 2 Choose **User Groups** from the navigation pane, and click **Create User Group** in the upper right corner.

Figure 4-1 Creating a user group



Step 3 On the displayed page, enter a user group name.

Step 4 Click **OK**.

NOTE

You can create a maximum of 20 user groups. To create more user groups, increase the quota by referring to **How Do I Increase My Quota?**

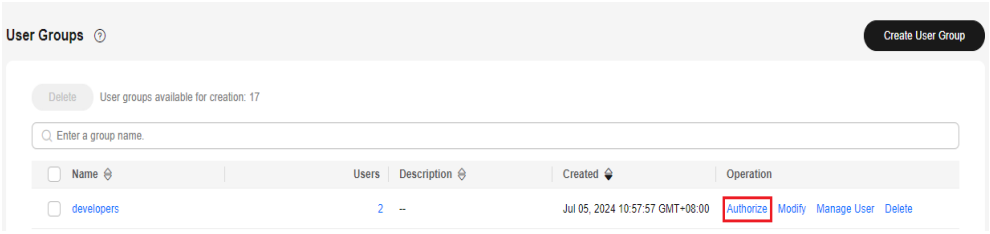
----End

Assigning Permissions to a User Group

To assign permissions to a user group, perform the operations below. To revoke permissions of a user group, see **Managing Permissions of a User Group**.

Step 1 In the user group list, locate the created user group click **Authorize** in the **Operation** column.

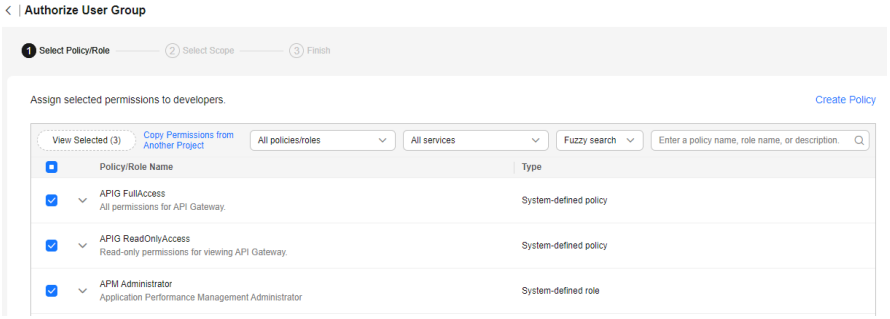
Figure 4-2 Going to the user group authorization page



Step 2 On the **Authorize User Group** page, select the permissions to be assigned to the user group and click **Next**.

If the system-defined policies do not meet your requirements, click **Create Policy** in the upper right corner to create custom policies. You can use them to supplement system-defined policies for refined permissions control. For details, see **Creating a Custom Policy**.

Figure 4-3 Selecting permissions



Step 3 Specify the scope. The system automatically recommends an authorization scope for the permissions you selected. **Table 4-1** describes all the authorization scopes provided by IAM.

Table 4-1 Authorization scopes

Scope	Description
All resources	IAM users will be able to use all resources, including those in enterprise projects, region-specific projects, and global services under your account based on assigned permissions.
Enterprise projects	IAM users can use the resources in the enterprise projects you select based on the assigned permissions. This option is available only when Enterprise Project is enabled. For details about enterprise projects, see **What Is Enterprise Project Management Service?**. To enable Enterprise Project, see **Enabling the Enterprise Project Function**.

Scope	Description
Region-specific projects	IAM users can use the resources in the region-specific projects you select based on the assigned permissions. If you select global service permissions, the permissions will be applied to all resources by default. If you select project-level service permissions, the permissions will be applied to the region-specific projects you select. **NOTE** The region-specific projects for Dedicated Cloud cannot be selected.
Global services	IAM users can use global services based on the assigned permissions. Global services are deployed for all physical regions. IAM users do not need to specify a region when accessing these services, such as Object Storage Service (OBS) and Content Delivery Network (CDN). If you select project-level service permissions, the permissions will be applied to all resources by default. If you select global service permissions, the permissions will be applied to the global services.

Step 4 Click **OK**.

----End

Table 4-2 lists the common permissions. For all service-specific permissions, see **System-defined Permissions**.

NOTE

- If you add an IAM user to multiple groups, the user will inherit all the permissions from these groups.
- For more information about permissions management, see **Assigning Permissions to O&M Personnel**, **Assigning Dependency Roles**, and **Custom Policy Examples**.
- In the enterprise project authorization, if OBS permissions are assigned, they will be applied about 15 to 30 minutes after the authorization is complete.

Table 4-2 Common permissions

Category	Policy/Role Name	Description	Authorization Scope
General administration	FullAccess	Full permissions for services supporting policy-based access control.	All resources
Resource management	Tenant Administrator	Administrator permissions for all services except IAM.	All resources
Viewing resources	Tenant Guest	Read-only permissions for all resources.	All resources

Category	Policy/Role Name	Description	Authorization Scope
IAM user management	Security Administrator	Administrator permissions for IAM.	Global services
Accounting management	BSS Administrator	Administrator permissions for Billing Center, including managing invoices, orders, contracts, and renewals, and viewing bills. **NOTE** The **BSS Administrator** permissions need to be assigned for all regions.	Region-specific projects
Computing O&M	ECS FullAccess	Administrator permissions for Elastic Cloud Server (ECS).	Region-specific projects
	CCE FullAccess	Administrator permissions for Cloud Container Engine (CCE).	Region-specific projects
	CCI FullAccess	Administrator permissions for Cloud Container Instance (CCI).	Region-specific projects
	BMS FullAccess	Administrator permissions for Bare Metal Server (BMS).	Region-specific projects
	IMS FullAccess	Administrator permissions for Image Management Service (IMS).	Region-specific projects
	AutoScaling FullAccess	Administrator permissions for Auto Scaling (AS).	Region-specific projects
Network O&M	VPC FullAccess	Administrator permissions for Virtual Private Cloud (VPC).	Region-specific projects
	ELB FullAccess	Administrator permissions for Elastic Load Balance (ELB).	Region-specific projects

Category	Policy/Role Name	Description	Authorization Scope
Database O&M	RDS FullAccess	Administrator permissions for Relational Database Service (RDS).	Region-specific projects
	DDS FullAccess	Administrator permissions for Document Database Service (DDS).	Region-specific projects
	DDM FullAccess	Administrator permissions for Distributed Database Middleware (DDM).	Region-specific projects
Security O&M	Anti-DDoS Administrator	Administrator permissions for Anti-DDoS.	Region-specific projects
	AAD Administrator	Administrator permissions for Advanced Anti-DDoS (AAD).	Region-specific projects
	WAF Administrator	Administrator permissions for Web Application Firewall (WAF).	Region-specific projects
	VSS Administrator	Administrator permissions for Vulnerability Scan Service (VSS).	Region-specific projects
	CGS Administrator	Administrator permissions for Container Guard Service (CGS).	Region-specific projects
	KMS Administrator	Administrator permissions for Key Management Service (KMS), which has been renamed Data Encryption Workshop (DEW).	Region-specific projects
	DBSS System Administrator	Administrator permissions for Database Security Service (DBSS).	Region-specific projects

Category	Policy/Role Name	Description	Authorization Scope
	SES Administrator	Administrator permissions for Security Expert Service (SES).	Region-specific projects
	SC Administrator	Administrator permissions for SSL Certificate Manager (SCM).	Region-specific projects

Related Operations

Huawei Cloud services interwork with each other, and some cloud services are dependent on other services. Roles of these services take effect only if they are assigned along with the dependency roles. Policies, however, do not require dependencies.

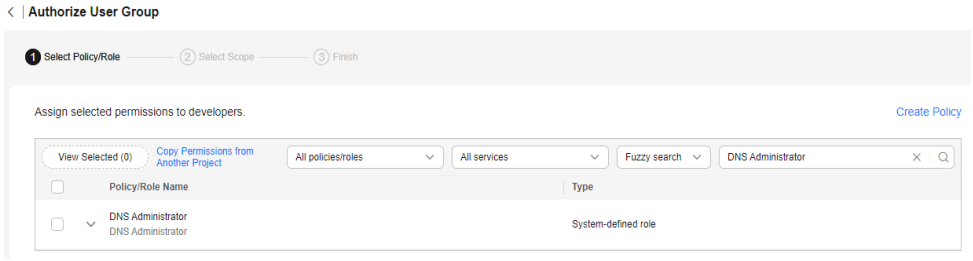
Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user group list, click **Authorize** in the row that contains the created user group.

Step 3 On the displayed page, search for a role in the search box in the upper right corner.

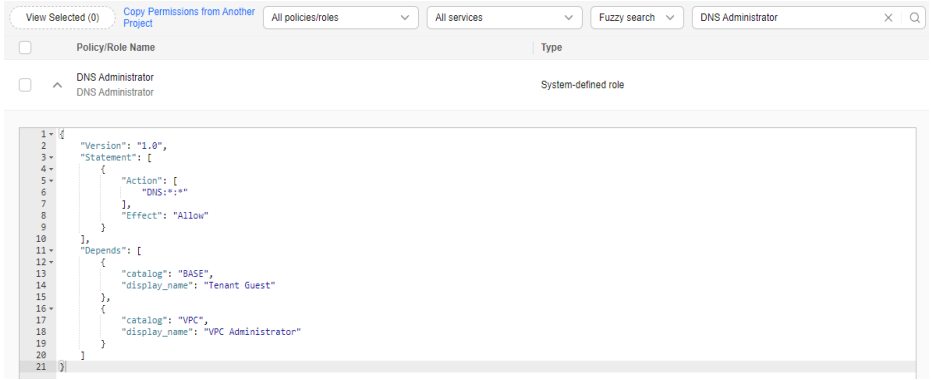
Step 4 Select the target role. The system automatically selects the dependency roles.

Figure 4-4 Selecting a role



Step 5 Click ⌄ in front of the role to view the dependencies.

Figure 4-5 Viewing dependencies



For example, the **DNS Administrator** role contains the **Depends** parameter which specifies the dependency roles. When you assign the **DNS Administrator** role to a user group, you also need to assign the **Tenant Guest** and **VPC Administrator** roles to the group for the same project.

Step 6 Click **OK**.

----End

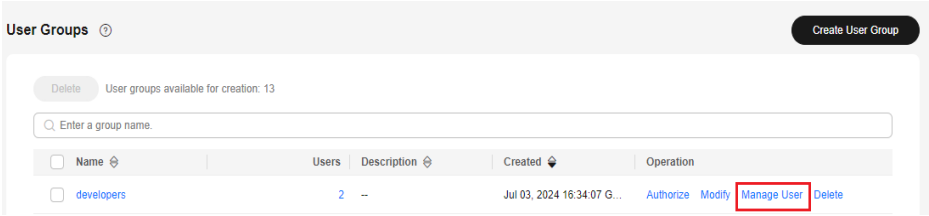
4.3 Adding IAM Users to or Removing IAM Users from a User Group

A user inherits permissions from the groups which the user belongs to. To change the permissions of a user, add the user to a new group or remove the user from an existing group.

Adding Users to a User Group

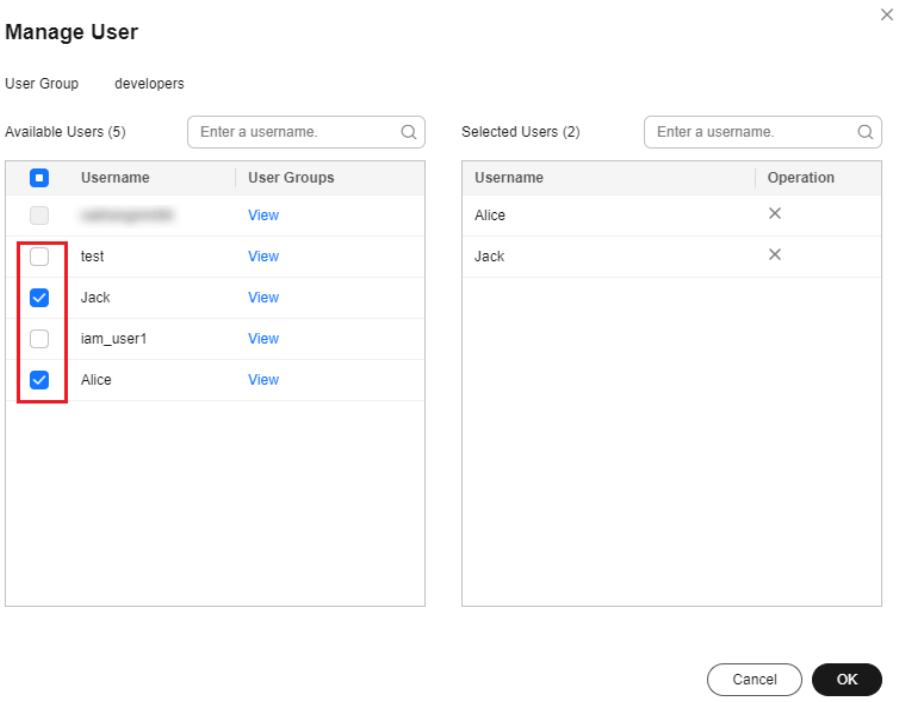
Step 1 In the user group list, click **Manage User** in the row containing the target user group.

Figure 4-6 Managing group membership



Step 2 In the **Manage User** dialog box, select the usernames to be added.

Figure 4-7 Selecting users



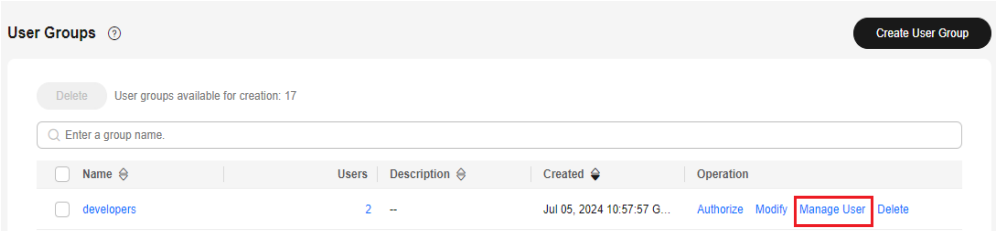
Step 3 Click **OK**.

----End

Removing Users from a User Group

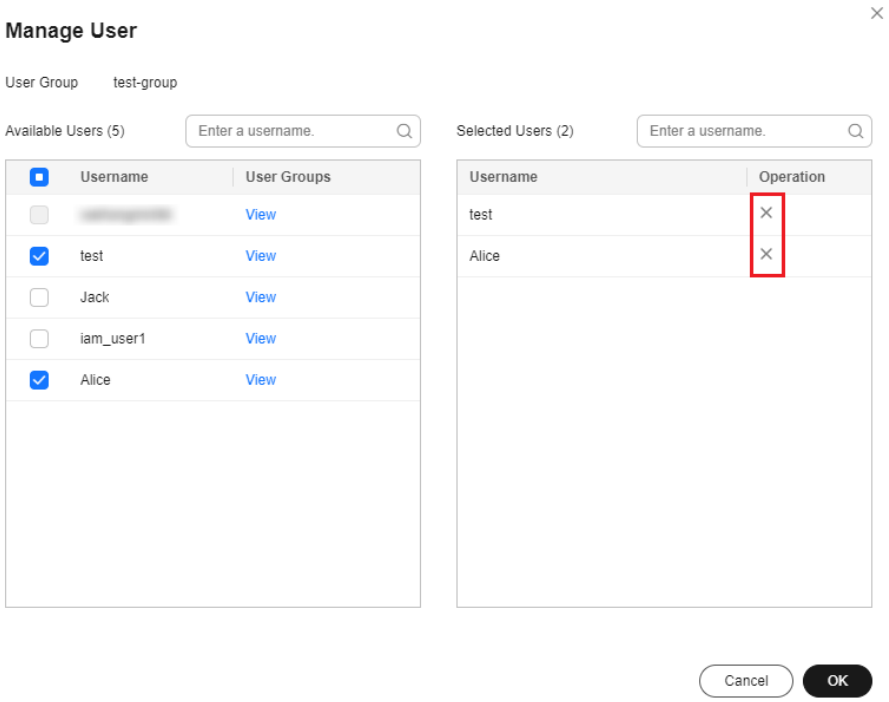
Step 1 In the user group list, click **Manage User** in the row containing the target user group.

Figure 4-8 Managing group membership



Step 2 In the **Selected Users** area, locate the user to be removed and click the **×**. Then, click **OK**.

Figure 4-9 Removing users from a user group



----End

4.4 Deleting User Groups

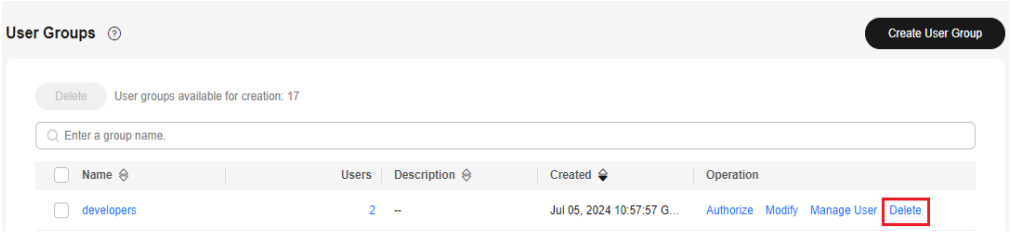
Procedure

To delete a user group, do the following:

Step 1 Log in to the **IAM console**. In the navigation pane, choose **User Groups**.

Step 2 In the user group list, click **Delete** in the row that contains the user group to be deleted.

Figure 4-10 Deleting a user group



Step 3 In the displayed dialog box, click **OK**.

----End

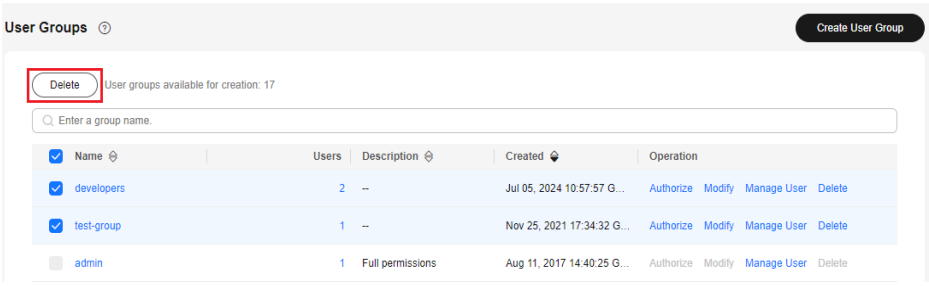
Batch Deleting User Groups

To delete multiple user groups at a time, do the following:

Step 1 Log in to the **IAM console**. In the navigation pane, choose **User Groups**.

Step 2 In the user group list, select the user groups to be deleted and click **Delete** above the list.

Figure 4-11 Batch deleting user groups



Step 3 In the displayed dialog box, click **OK**.

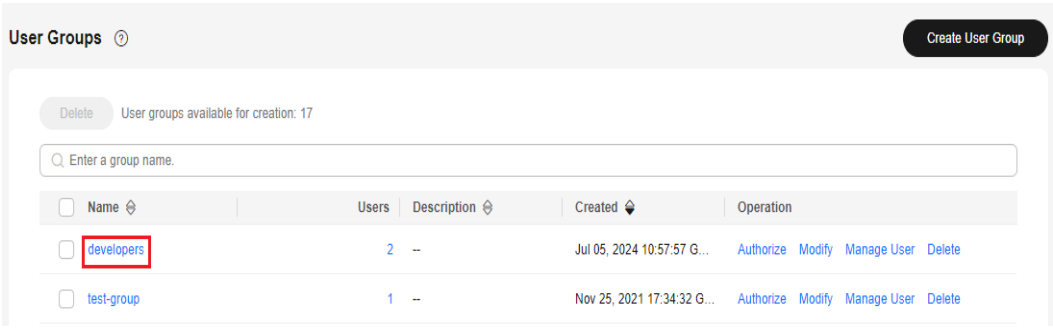
----End

4.5 Managing User Group Information

Viewing User Group Information

In the user group list, click the user group name to view its basic information, assigned permissions, and managed users.

Figure 4-12 Viewing user group information



Modifying a User Group Name and Description

In the user group list, click **Modify** in the row containing the user group whose name and description you want to modify, and modify the name and description.

Figure 4-13 Modifying the user group name and description

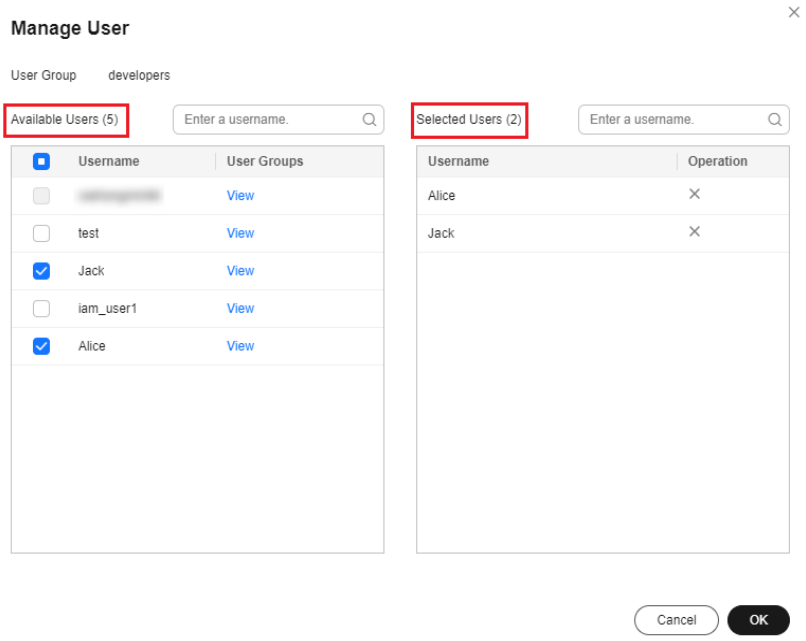
NOTE

If a user group name has been configured in the identity conversion rules of an identity provider, modifying the user group name will cause the identity conversion rules to fail. Exercise caution when performing this operation.

Managing Users in a Group

Step 1 In the user group list, click **Manage User** in the row containing the user group you want to modify.

Figure 4-14 Managing users in the group



Step 2 In the **Available Users** area, select users you want to add to the user group.

Step 3 In the **Selected Users** area, remove users from the user group.

----End

NOTE

For the default group **admin**, you can only manage its users and cannot modify its description or permissions.

4.6 Managing Permissions of a User Group

You can modify or delete permissions of a user group on its details page.

Modifying User Group Permissions

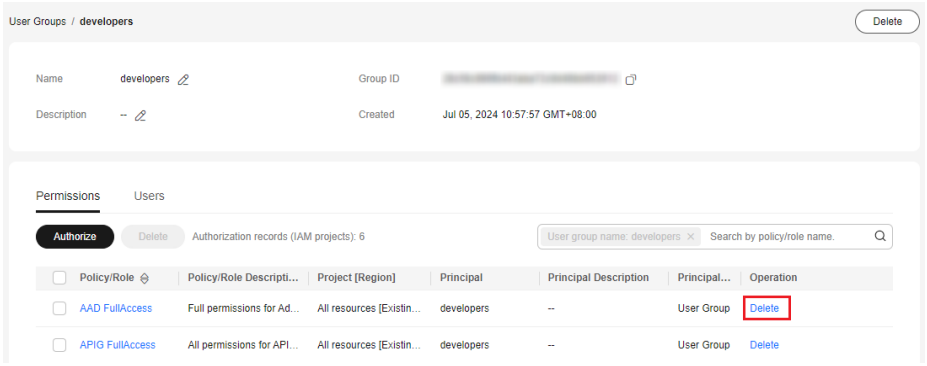
You can view or modify user group permissions on the **Permissions** page of the IAM console.

NOTE

- Modifying the permissions of a user group affects the permissions of all users in the user group.
- Permissions of the default user group **admin** cannot be modified.

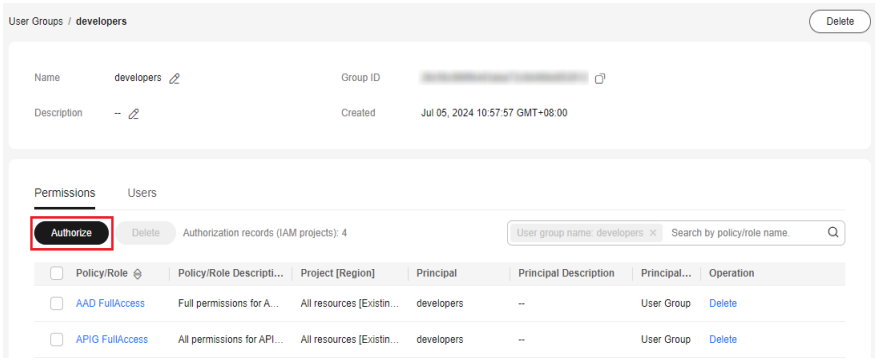
1. Click a user group (for example, the developer group) to go to the details page, and view the group permissions on the **Permissions** tab.
2. Click **Delete** in the row that contains the role or policy you want to delete.

Figure 4-15 Deleting an assigned permission



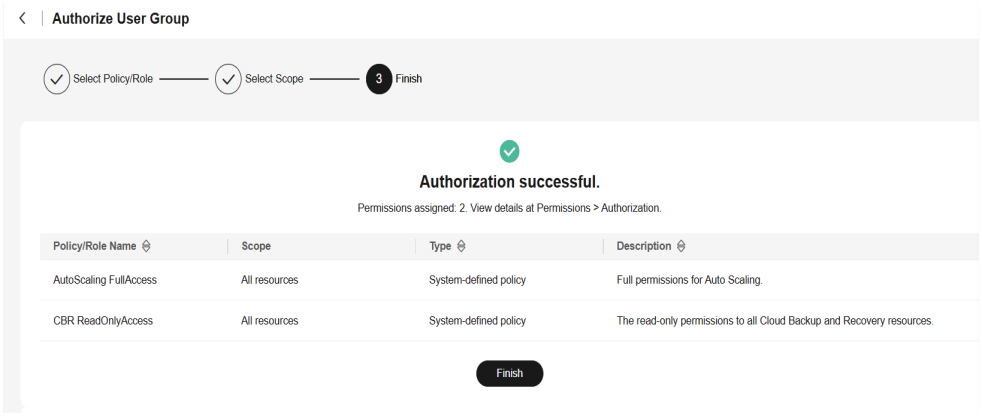
3. Click **OK**.
4. On the **Permissions** tab, click **Authorize**.

Figure 4-16 Assigning permissions to a user group



5. Select desired permissions and a scope, and click **OK**.
6. Go back to the **Permissions** tab to view the modified group permissions.

Figure 4-17 Permissions assigned



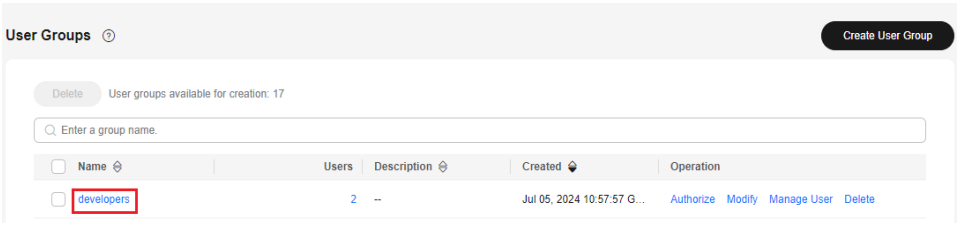
Revoking Permissions of a User Group

To revoke a policy or role attached to a user group, do the following:

Step 1 Log in to the **IAM console**. In the navigation pane, choose **User Groups**.

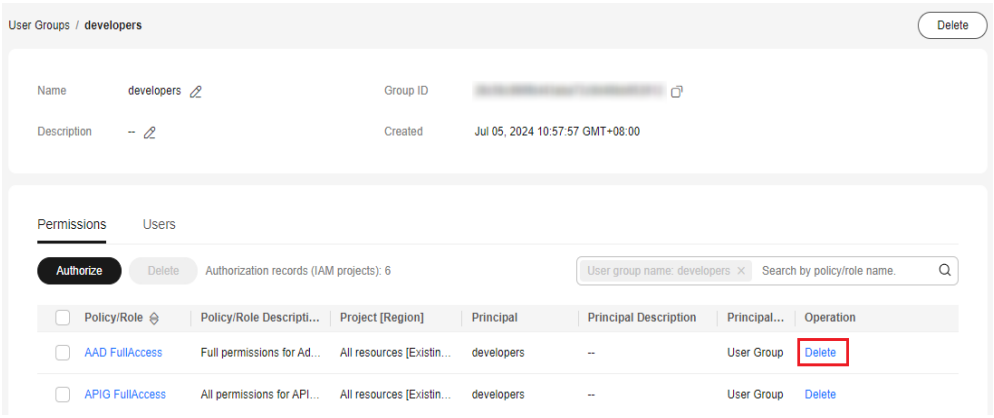
Step 2 Click the name of the user group to go to the group details page.

Figure 4-18 Clicking a user group name



Step 3 On the **Permissions** tab, click **Delete** in the row that contains the role or policy you want to delete.

Figure 4-19 Revoking permissions



Step 4 In the displayed dialog box, click **OK**.

----End

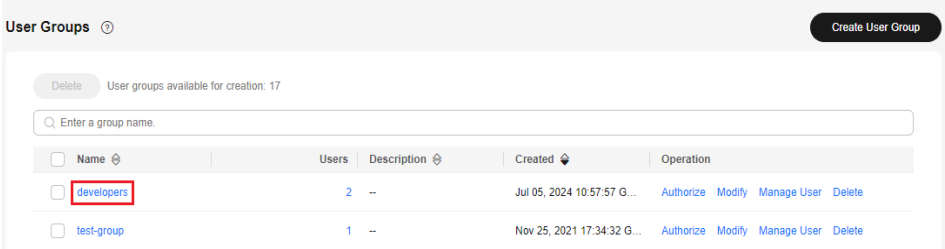
Batch Deleting Permissions of a User Group

To revoke multiple policies or roles attached to a user group, do as follows:

Step 1 Log in to the **IAM console**. In the navigation pane, choose **User Groups**.

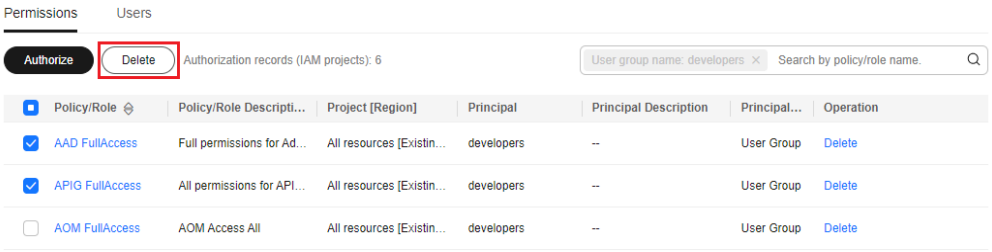
Step 2 Click the name of the user group to go to the group details page.

Figure 4-20 Viewing a user group



Step 3 On the **Permissions** page, select the roles or policies you want to delete and click **Delete** above the list.

Figure 4-21 Batch deleting permissions



Step 4 In the displayed dialog box, click **OK**.

----End

4.7 Assigning Dependency Roles

Huawei Cloud services interwork with each other. Roles of some services take effect only if they are assigned along with roles of other services.

Procedure

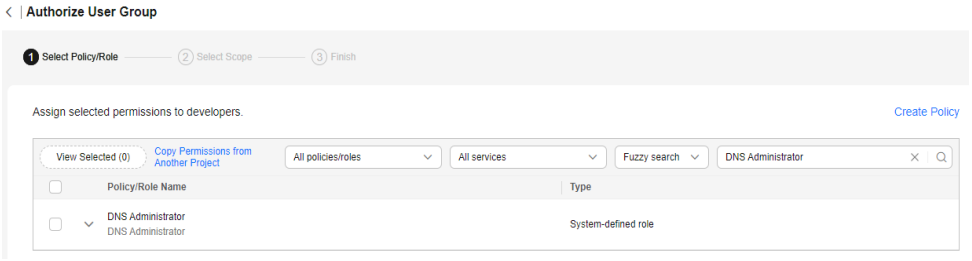
Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user group list, click **Authorize** in the row that contains the created user group.

Step 3 On the displayed page, search for a role in the search box in the upper right corner.

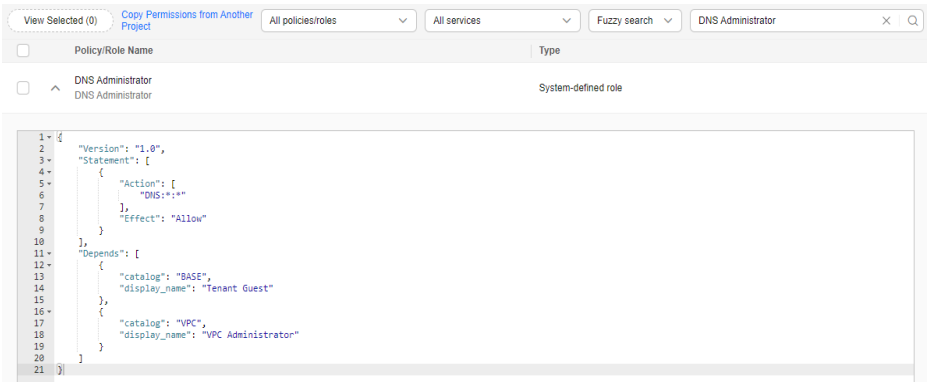
Step 4 Select the target role. The system automatically selects the dependency roles.

Figure 4-22 Selecting a role



Step 5 Click ⌄ next to the role to view the dependencies.

Figure 4-23 Viewing dependencies



For example, the **DNS Administrator** role contains the **Depends** parameter which specifies the dependency roles. When you assign the **DNS Administrator** role to a user group, you also need to assign the **Tenant Guest** and **VPC Administrator** roles to the group for the same project.

Step 6 Click **OK**.

----End

5 Permissions Management

5.1 Basic Concepts

5.1.1 Basic Concepts

Permission

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and then attach policies or roles to these groups. The users then inherit permissions from the user group and can perform specified operations on cloud services.

Permission Type

You can grant permissions by using roles and policies.

- **Roles**: A coarse-grained authorization strategy that defines permissions by job responsibility. Only a limited number of service-level roles are available for authorization. When using roles to grant permissions, you also need to assign dependency roles. Roles are not ideal for fine-grained authorization and least privilege access.
- **Policies**: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only the permissions required to manage ECSs of a certain type.

  IAM supports both **system-defined policies** and **custom policies**.

System-Defined Policy

A system-defined policy defines the common actions of a cloud service. System-defined policies can be used to assign permissions to user groups, and they cannot be modified. For details about the system-defined policies of all cloud services, see **System-defined Permissions**.

If there are no system-defined policies for a specific service, it indicates that IAM does not support this service. You can **submit a service ticket** and apply for permissions management on IAM.

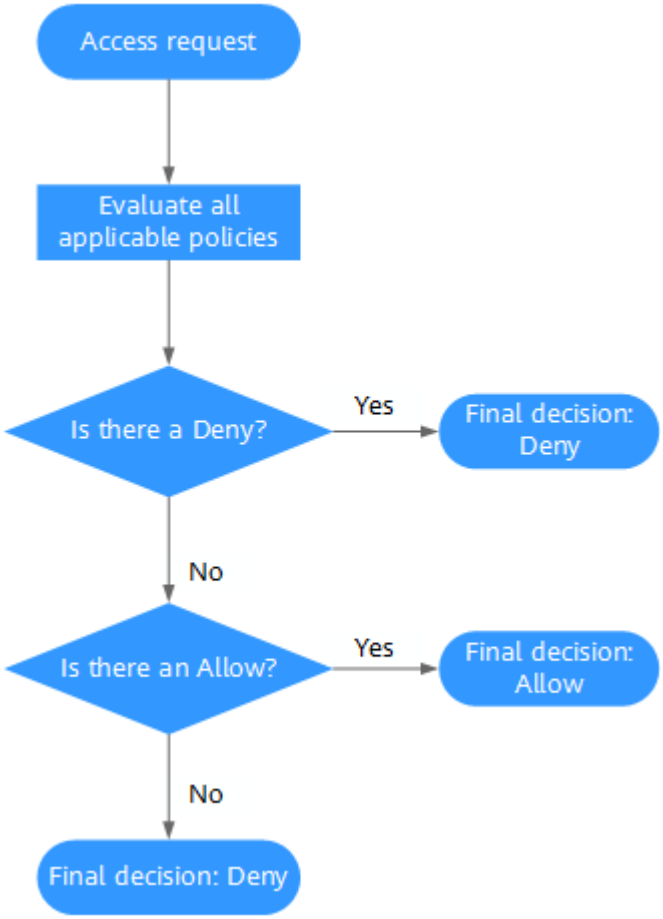
Custom Policy

You can create custom policies using the actions supported by cloud services to supplement system-defined policies for more refined access control. You can create custom policies in visual editor or JSON view.

Authentication Process

When a user initiates an access request, the system authenticates the request based on the actions in the policies that have been attached to the group that the user belongs to. The following diagram shows the authentication process.

Figure 5-1 Authentication process



1. A user initiates an access request.
2. The system looks for a Deny among the applicable actions of the policies from which the user gets permissions. If the system finds an applicable Deny, it returns a decision of Deny, and the authentication ends.

3. If no Deny is found applicable, the system looks for an Allow that would apply to the request. If the system finds an applicable Allow, it returns a decision of Allow, and the authentication ends.
4. If no Allow is found applicable, the system returns a decision of Deny, and the authentication ends.

5.1.2 Changes to the System-defined Policy Names

All the system-defined policies (previously called "fine-grained policies") have been renamed and the new names are effective from Feb 6, 2020 22:30:00 GMT +08:00. This change does not affect your services. The original system-defined policies are Version 1.0, and the new system-defined policies are Version 1.1. IAM is compatible with both versions.

Table 5-1 Original and current system-defined policy names

Service	Original	Current
AOM	AOM Admin	AOM FullAccess
	AOM Viewer	AOM ReadOnlyAccess
APM	APM Admin	APM FullAccess
	APM Viewer	APM ReadOnlyAccess
Auto Scaling	AutoScaling Admin	AutoScaling FullAccess
	AutoScaling Viewer	AutoScaling ReadOnlyAccess
BMS	BMS Admin	BMS FullAccess
	BMS User	BMS CommonOperations
	BMS Viewer	BMS ReadOnlyAccess
BSS	EnterpriseProject_BSS_Administrator	EnterpriseProject BSS FullAccess
CBR	CBR Admin	CBR FullAccess
	CBR User	CBR BackupsAndVaults-FullAccess
	CBR Viewer	CBR ReadOnlyAccess
CCE	CCE Admin	CCE FullAccess
	CCE Viewer	CCE ReadOnlyAccess
CCI	CCI Admin	CCI FullAccess
	CCI Viewer	CCI ReadOnlyAccess
CDM	CDM Admin	CDM FullAccess

Service	Original	Current
	CDM Operator	CDM FullAccessExcep-tUpdateEIP
	CDM Viewer	CDM ReadOnlyAccess
	CDM User	CDM CommonOperations
CDN	CDN Domain Configuration Operator	CDN DomainConfigureAccess
	CDN Domain Viewer	CDN DomainReadOnlyAccess
	CDN Logs Viewer	CDN LogsReadOnlyAccess
	CDN Refresh And Preheat Operator	CDN RefreshAndPrehea-tAccess
	CDN Statistics Viewer	CDN StatisticsReadOn-lyAccess
CES	CES Admin	CES FullAccess
	CES Viewer	CES ReadOnlyAccess
CS	CS Admin	CS FullAccess
	CS Viewer	CS ReadOnlyAccess
	CS User	CS CommonOperations
CSE	CSE Admin	CSE FullAccess
	CSE Viewer	CSE ReadOnlyAccess
DCS	DCS Admin	DCS FullAccess
	DCS Viewer	DCS ReadOnlyAccess
	DCS User	DCS UseAccess
DDM	DDM Admin	DDM FullAccess
	DDM Viewer	DDM ReadOnlyAccess
	DDM User	DDM CommonOperations
DDS	DDS Admin	DDS FullAccess
	DDS DBA	DDS ManageAccess
	DDS Viewer	DDS ReadOnlyAccess
DLF	DLF Admin	DLF FullAccess

Service	Original	Current
	DLF Developer	DLF Development
	DLF Operator	DLF OperationAndMaintenanceAccess
	DLF Viewer	DLF ReadOnlyAccess
DMS	DMS Admin	DMS FullAccess
	DMS Viewer	DMS ReadOnlyAccess
	DMS User	DMS UseAccess
DNS	DNS Admin	DNS FullAccess
	DNS Viewer	DNS ReadOnlyAccess
DSS	DSS Admin	DSS FullAccess
	DSS Viewer	DSS ReadOnlyAccess
DWS	DWS Admin	DWS FullAccess
	DWS Viewer	DWS ReadOnlyAccess
ECS	ECS Admin	ECS FullAccess
	ECS Viewer	ECS ReadOnlyAccess
	ECS User	ECS CommonOperations
ELB	ELB Admin	ELB FullAccess
	ELB Viewer	ELB ReadOnlyAccess
EPS	EPS Admin	EPS FullAccess
	EPS Viewer	EPS ReadOnlyAccess
EVS	EVS Admin	EVS FullAccess
	EVS Viewer	EVS ReadOnlyAccess
GES	GES Admin	GES FullAccess
	GES Viewer	GES ReadOnlyAccess
	GES User	GES Development
ICITY	iCity Admin	iCity FullAccess
	iCity Viewer	iCity ReadOnlyAccess
IMS	IMS Admin	IMS FullAccess
	IMS Viewer	IMS ReadOnlyAccess
Image Recognition	Image Recognition User	Image Recognition FullAccess

Service	Original	Current
KMS	DEW Keypair Admin	DEW KeypairFullAccess
	DEW Keypair Viewer	DEW KeypairReadOnlyAccess
	KMS CMK Admin	KMS CMKFullAccess
LTS	LTS Admin	LTS FullAccess
	LTS Viewer	LTS ReadOnlyAccess
MRS	MRS Admin	MRS FullAccess
	MRS Viewer	MRS ReadOnlyAccess
	MRS User	MRS CommonOperations
ModelArts	ModelArts Admin	ModelArts FullAccess
	ModelArts User	ModelArts CommonOperations
Moderation	Moderation User	Moderation FullAccess
NAT	NAT Admin	NAT FullAccess
	NAT Viewer	NAT ReadOnlyAccess
OBS	OBS Operator	OBS OperateAccess
	OBS Viewer	OBS ReadOnlyAccess
RDS	RDS Admin	RDS FullAccess
	RDS DBA	RDS ManageAccess
	RDS Viewer	RDS ReadOnlyAccess
RES	RES Admin	RES FullAccess
	RES Viewer	RES ReadOnlyAccess
ROMA Connect	ROMA Admin	ROMA FullAccess
	ROMA Viewer	ROMA ReadOnlyAccess
SCM	SCM Admin	SCM FullAccess
	SCM Viewer	SCM ReadOnlyAccess
	SCM Viewer	SCM ReadOnlyAccess
SFS	SFS Admin	SFS FullAccess
	SFS Viewer	SFS ReadOnlyAccess
SFS Turbo	SFS Turbo Administrator	SFS Turbo FullAccess

Service	Original	Current
	SFS Turbo Viewer	SFS Turbo ReadOnlyAccess
ServiceStage	ServiceStage Admin	ServiceStage FullAccess
	ServiceStage Developer	ServiceStage Development
	ServiceStage Viewer	ServiceStage ReadOnlyAccess
VPC	VPC Admin	VPC FullAccess
	VPC Viewer	VPC ReadOnlyAccess

5.1.3 Role Syntax

Roles are a coarse-grained authorization strategy that defines permissions by job responsibility. Only a limited number of service-level roles are available for authorization. Roles are not ideal for fine-grained authorization and least privilege access.

Huawei Cloud services often depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. For more information, see **Assigning Dependency Roles**.

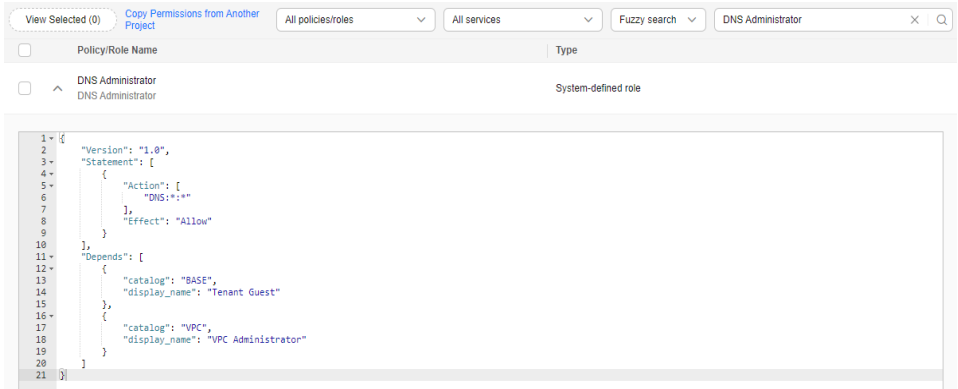
Constraints

Roles cannot be used for permissions assignment in enterprise project authorization.

Role Content

When using roles to assign permissions, you can select a role and click ⌄ to view the details of the role. This section uses the **DNS Administrator** role as an example to describe the role content.

Figure 5-2 Content of the DNS Administrator role




```
{
   "Version": "1.0",
   "Statement": [
      {
         "Action": [
            "DNS:Zone:*",
            "DNS:RecordSet:*",
            "DNS:PTRRecord:*"
         ],
         "Effect": "Allow"
      }
   ],
   "Depends": [
      {
         "catalog": "BASE",
         "display_name": "Tenant Guest"
      },
      {
         "catalog": "VPC",
         "display_name": "VPC Administrator"
      }
   ]
}
```

Parameter Description

Table 5-2 Parameter description

Parameter		Description	Value
Version		Role version.	**1.0**: indicates role-based access control.
Statement	Action	Operations to be performed on the service.	Format: "*Service name*:*Resource type*:*Operation*". **DNS:Zone:***: Permissions for performing all operations on Domain Name Service (DNS) zones.
	Effect	Determines whether to allow or deny the operations defined in the action.	• Allow • Deny **NOTE** If an action has both Allow and Deny effects, the Deny effect takes precedence.
Depends	catalog	Name of the service to which a dependency role belongs.	Service name. Example: **BASE** and **VPC**.

Parameter		Description	Value
	display_name	Name of the dependency role.	Role name. **NOTE** When you assign the **DNS Administrator** role to a user group, you also need to assign the **Tenant Guest** and **VPC Administrator** roles to the group for the same project. For more information about dependencies, see **System-defined Permissions**.

5.1.4 Policy Syntax

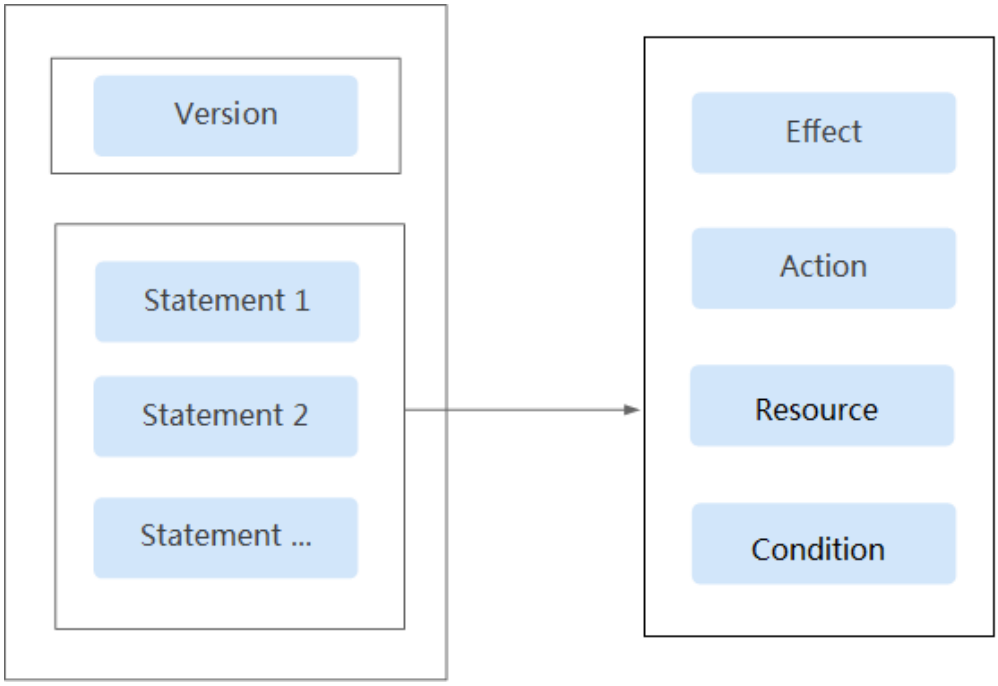
The following uses a custom policy for OBS as an example to describe the policy syntax.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "obs:bucket:ListAllMyBuckets",
            "obs:bucket:HeadBucket",
            "obs:bucket:ListBucket",
            "obs:bucket:GetBucketLocation"
         ],
         "Condition": {
            "StringEndWithIfExists": {
               "g:UserName": [
                  "specialCharacter"
               ]
            },
            "Bool": {
               "g:MFAPresent": [
                  "true"
               ]
            }
         },
         "Resource": [
            "obs:*:*:bucket:*"
         ]
      }
   ]
}
```

Policy Structure

A policy consists of a version and one or more statements (indicating different actions).

Figure 5-3 Policy structure



Policy Parameters

Policy parameters include **Version** and **Statement**, which are described in the following table. You can create custom policies by specifying the parameters. For details, see **Custom Policy Examples**.

Table 5-3 Policy parameters

Parameter		Description	Value
Version		Policy version.	**1.1**: indicates policy-based access control.
Statement	Effect	Determines whether to allow or deny the operations defined in the action.	• Allow • Deny **NOTE** If an action has both Allow and Deny effects, the Deny effect takes precedence.

Parameter		Description	Value
	Action	Operations to be performed on the service.	Format: "*Service name*:*Resource type*:*Operation*". Wildcard characters (*) are supported, indicating all options. Actions are case insensitive. Example: **obs:bucket:ListAllMybuckets**: Permissions for listing all OBS buckets. View all actions of the service in its *API Reference*, for example, see **Supported Actions of OBS**.
	Condition	Determines when a policy takes effect. A condition consists of a **condition key** and an **operator**.	Format: "*Condition operator*:{*Condition key*:[*Value 1*,*Value 2*]}" (the condition key is case insensitive) If you set multiple conditions, the policy takes effect only when all the conditions are met. Example: **StringEndWithIfExists": {"g:UserName": ["specialCharacter"]}**: The statement is valid for users whose names end with **specialCharacter**.
	Resource	Resources on which the policy takes effect.	Format: *Service name*:*region*:*domainId*:*Resource type*:*Resource path*. The resource type is case insensitive. It supports wildcard characters (*), which indicates all resources. For details about cloud services that support resource-level authorization and supported resource types, see **Cloud Services that Support Resource-Level Authorization Using IAM**. Example: • **obs:*:*:bucket:***: All OBS buckets. • **obs:*:*:object:my-bucket/my-object/***: All objects in the **my-object** directory of the **my-bucket** bucket.

- **Condition key**

  A condition key is a key in the Condition element of a statement. There are global and service-level condition keys.

  - Global condition keys (starting with **g:**) apply to all operations. IAM provides **common global condition keys** and **special global condition keys**.
    - Common global condition keys: Cloud services do not need to provide user identity information. Instead, IAM automatically abstracts user information and authenticates users. For details, see **Table 5-4**.
    - Special global condition keys: IAM obtains condition information from cloud services for authentication. Only certain cloud services support special global condition keys.
  - Service-level condition keys (starting with a service name abbreviation, for example, **obs:**) apply only to operations on the specified service. For details, see the user guide of the corresponding cloud service, for example, see **OBS Request Conditions**.

Table 5-4 Common global condition keys

Global Condition Key	Type	Description
g:CurrentTime	Time	Time when an authentication request is received. The time is in ISO 8601 format, for example, **2012-11-11T23:59:59Z**. (See an example in **a**.)
g:DomainName	String	Account name of the requester. (See an example in **b**.)
g:MFAPresent	Boolean	Whether to obtain a token through MFA authentication. (See an example in **3**.)
g:MFAAge	Number	Validity period of a token obtained through MFA authentication. This condition must be used together with **g:MFAPresent**. (See an example in **d**.)
g:PKITokenIssueTime	Time	Time when the PKI token is issued. The time is in ISO 8601 format, for example, 2012-11-11T23:59:59Z. (See an example in **e**.)
g:ProjectName	String	Project name. (See an example in **f**.)
g:UserId	String	IAM user ID. (See an example in **g**.)
g:UserName	String	IAM username. (See an example in **h**.)

Table 5-5 Special global condition keys

Global Condition Key	Type	Description
g:SourceIp	IP Address	IP address of the user sending a request.
g:SourceVpc	String	VPC ID of the user sending a request.
g:SourceVpce	String	VPC endpoint ID of the user sending a request.
g:TagKeys	String	Resource tag key.
g:ResourceTag/{TagKey}	String	Resource tag key value.

a. **g:CurrentTime**

Example: The following policy grants permission to create agencies in IAM from March 1, 2023, 08:00 GMT+08:00 to March 30, 2023, 08:00 GMT+08:00. The value of the **g:CurrentTime** condition key is in UTC format.

```
{
    "Version": "1.1",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iam:roles:createRoles"],
        "Condition": {
            "DateGreaterThan": {
                "g:CurrentTime": ["2023-03-01T00:00:00Z"]
            },
            "DateLessThan": {
                "g:CurrentTime": ["2023-03-30T00:00:00Z"]
            }
        }
    }]
}
```

b. **g: DomainName**

Example: The following policy only allows user **zhangsan** to create agencies in IAM.

```
{
    "Version": "1.1",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iam:roles:createRoles"],
        "Condition": {
            "StringEquals": {
                "g:DomainName": ["zhangsan"]
            }
        }
    }]
}
```

c. **g:MFAPresent**

Example: The following policy allows users who obtain credentials using MFA to create agencies in IAM.


```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "Bool": {
                                "g:MFAPresent": ["true"]
                        }
                }
        }]
}
```

d. **g:MFAAge**

Example: The following policy allows users who obtain credentials using MFA with the valid period greater than 900s to create agencies in IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        " NumberGreaterThanEquals ": {
                                "g:MFAAge": ["900"]
                        }
                }
        }]
}
```

e. **g:PKITokenIssueTime**

Example: The following policy allows users who use the PKI token issued before March 1 08:00, 2023 (Beijing Time) to create agencies in IAM.

NOTE

The value of the **g:PKITokenIssueTime** condition key is in UTC format.

```
{
   "Version": "1.1",
   "Statement": [{
      "Effect": "Allow",
      "Action": ["iam:roles:createRoles"],
      "Condition": {
         "DateLessThan": {
            "g:PKITokenIssueTime": ["2023-03-01T00:00:00Z"]
         }
      }
   }]
}
```

f. **g:ProjectName**

Example: The following policy allows users who obtain credentials in **CN North-Beijing** to create agencies in IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        " StringEquals ": {
                                "g: ProjectName ": ["cn-north-4"]
                        }
                }
        }]
}
```

g. **g: UserId**

Example: The following policy allows user whose ID is **xxxxxxxxxxx...** to create agencies in IAM.

```
{
	"Version": "1.1",
	"Statement": [{
		"Effect": "Allow",
		"Action": ["iam:roles:createRoles"],
		"Condition": {
			"StringEquals": {
				"g: UserId ": ["xxxxxxxxxxx..."]
			}
		}
	}]
}
```

h. **g: UserName**

Example: The following policy allows user **lisi** to create agencies in IAM.

```
{
	"Version": "1.1",
	"Statement": [{
		"Effect": "Allow",
		"Action": ["iam:roles:createRoles"],
		"Condition": {
			"StringEquals": {
				"g: UserName ": ["lisi"]
			}
		}
	}]
}
```

– Multivalued condition keys

i. ForAllValues: Tests whether the value of every member of the request set is a subset of the condition key set. The condition returns true if every key value in the request matches at least one value in the policy.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ims:images:share"
         ],
         "Condition": {
            "ForAllValues:StringEquals": {
               "ims:TargetOrgPaths": [
                  "orgPath1",
                  "orgPath2",
                  "orgPath3"
               ]
            }
         }
      }
   ]
}
```

This policy shows how to use the ForAllValues qualifier with the StringEquals condition operator. The condition determines whether to allow sharing with the member accounts in organization path orgPath1, orgPath2, or orgPath3.

Assume a user makes a request to share IMS with the member accounts in organization paths orgPath1 and orgPath3. The request is allowed because the user's requested attributes all match values specified in the policy.

If the user's request includes orgPath1, orgPath2, orgPath3, and orgPath4, the request fails because orgPath4 is not included in the condition operator.

ii. ForAnyValue: Tests whether at least one member of the set of request values matches at least one member of the set of condition key values. The condition returns true if any one of the key values in the request matches any one of the condition values in the policy. For no matching key or a null dataset, the condition returns false.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ims:images:share"
         ],
         "Condition": {
            "ForAnyValue:StringEquals": {
               "ims:TargetOrgPaths": [
                  "orgPath1",
                  "orgPath2",
                  "orgPath3"
               ]
            }
         }
      }
   ]
}
```

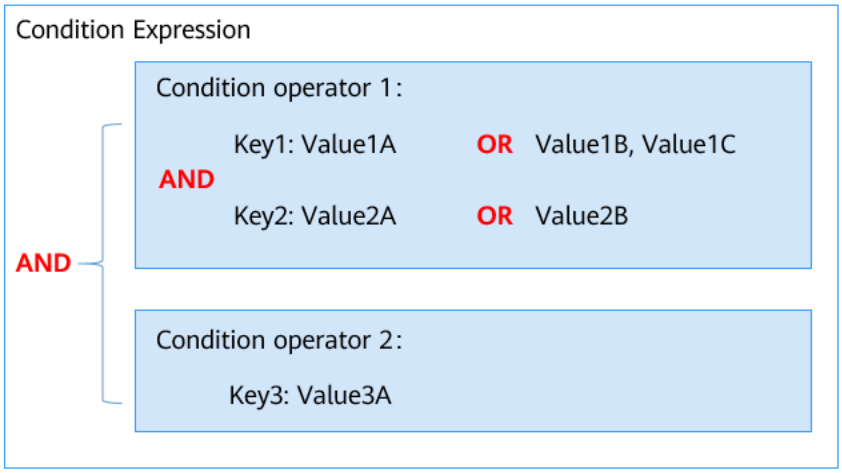
This policy shows how to use the ForAnyValue qualifier with the StringEquals condition operator. The condition determines whether to allow sharing with the member accounts in organization path orgPath1, orgPath2, or orgPath3.

Assume a user makes a request to share IMS with the member accounts in organization path orgPath1 or orgPath4. The request is allowed because the user's requested attributes all match values specified in the policy.

If the user initiates a request to share IMS with the member accounts in organization path orgPath4 or orgPath5, the request fails because orgPath4 and orgPath5 are not included in the condition operator.

Condition operators

Figure 5-4 Condition operators



a. If a single condition operator includes multiple values for one key, that condition operator is evaluated using a logical OR. The condition returns **true** if any one of the key values in the request matches any one of the condition values in the policy.

NOTICE

For negated matching condition operators (such as StringNotEquals), the request value cannot match any of the condition values based on the condition operators.

b. If your policy has multiple condition operators or multiple keys attached to a single condition operator, the conditions are evaluated using a logical AND.

- **Operator**

  An operator, a condition key, and a condition value together constitute a complete condition statement. A policy takes effect only when its request conditions are met. The operator suffix **IfExists** indicates that a policy takes effect if a request value is empty or meets the specified condition. For example, if the operator **StringEqualsIfExists** is selected for a policy, the policy takes effect if a request value is empty or equal to the specified condition value. Operators are string operators. They are not case-sensitive unless otherwise specified.

  – String condition operators

  Table 5-6 String condition operators

Type	Operator	Description
String	StringEquals	Exact matching, case sensitive
	StringNotEquals	Negated matching, case sensitive

Type	Operator	Description
	StringEqualsIgnore-Case	Exact matching
	StringNotEqualsIgnoreCase	Negated matching
	StringMatch	Case-sensitive matching. The values are regular expressions that support only multi-character match wildcards (*) and single-character match wildcards (?).
	StringNotMatch	Negated case-sensitive matching. The values are regular expressions that support only multi-character match wildcards (*) and single-character match wildcards (?).

For example, the following statement contains a Condition element that uses "g:DomainName" to specify that the principal whose domain name is "ZhangSan" can obtain the object content and metadata.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "obs:object:GetObject"
         ],
         "Condition": {
            "StringEquals": {
               "g:DomainName": [
                  "ZhangSan"
               ]
            }
         }
      }
   ]
}
```

– Numeric condition operators

Table 5-7 Numeric condition operators

Type	Operator	Description
Number	NumberEquals	Matching
	NumberNotEquals	Negated matching
	NumberLessThan	"Less than" matching
	NumberLessThanEquals	"Less than or equals" matching

Type	Operator	Description
	NumberGreaterThan	"Greater than" matching
	NumberGreaterThanEquals	"Greater than or equals" matching

For example, the following statement contains a Condition element that uses the "NumericLessThanEquals" condition operator with the "obs:max-keys" key to specify that the requester can list up to 10 objects in "example_bucket" at a time.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "obs:bucket:ListBucket"
         ],
         "Resource": [
            "OBS:*:*:bucket:example_bucket"
         ],
         "Condition": {
            "NumberLessThanEquals": {
               "obs:max-keys": [
                  "10"
               ]
            }
         }
      }
   ]
}
```

– Date condition operators

Table 5-8 Date condition operators

Type	Operator	Description
Date	DateLessThan	Matching before a specific date and time
	DateLessThanEquals	Matching at or before a specific date and time
	DateGreaterThan	Matching after a specific date and time
	DateGreaterThanEquals	Matching at or after a specific date and time

For example, the following statement contains a Condition element that uses the "DateLessThan" condition operator with the "g:CurrentTime" key to specify that the requester can create buckets only before August 1, 2022.

```
{
   "Version": "1.1",
```



```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:bucket:CreateBucket"
      ],
      "Condition": {
        "DateLessThan": {
          "g:CurrentTime": [
            "2022-08-01T00:00:00Z"
          ]
        }
      }
    }
  ]
}
```

- Bool condition operators

  Table 5-9 Bool condition operators

Type	Operator	Description
Bool	Bool	Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false."

  For example, the following policy allows only the requester with MFA enabled to modify specified permanent access keys.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:credentials:updateCredential"
      ],
      "Condition": {
        "Bool": {
          "g:MFAPresent": [
            "true"
          ]
        }
      }
    }
  ]
}
```

- Null condition operators

Table 5-10 Null condition operators

Type	Operator	Description
Null	Null	Use a Null condition operator to check if a condition key is absent at the time of authorization. In the policy statement, use either "true" (the key does not exist or is null) or "false" (the key exists and its value is not null).

For example, you can use this condition operator to specify that only requests of creating buckets from VPCs are allowed.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            " obs:bucket:CreateBucket"
         ],
         "Condition": {
            "Null": {
               "obs:SourceVpc": [
                  "false"
               ]
            }
         }
      }
   ]
}
```

– IfExists operator suffix

  You can add "IfExists" to the end of any condition operator name except the "Null condition", for example, StringEqualsIfExists. If the policy key is present in the context of the request, process the key as specified in the policy. If the key is not present, evaluate the Condition element as true.

5.1.5 Policy Variables

Introduction

When creating a custom policy, you can use policy variables as placeholders in the Resource or Condition element of a statement. When the policy is evaluated, these placeholders are automatically replaced with the values of the conditional context keys passed in the request.

Policy Variable Syntax and Replacement Rules

Policy variables are marked using a **$** prefix followed by a pair of curly braces (**{ }**). In the curly braces (**{ }**), enter the name of the target conditional context key passed in the request, for example, **${g:UserName}**. When the policy is evaluated, **${g:UserName}** is automatically replaced with the value of the **g:UserName** condition key.

NOTE

You can use a policy variable for Condition values in any position. The variable for the Resource element must appear in the fifth part separated by colons (:), for example, **OBS:*:*:bucket:${g:UserName}**.

If the specified conditional context key does not exist in the request or is a multivalued condition key, the replacement fails and the entire statement may be invalid. For example, the request contains the **g:UserName** condition key only when the principal is an IAM user. For other principals, the request does not contain the **g:UserName** condition key and therefore does not match any resource and condition key that contains **${g:UserName}**. Similarly, a multivalued condition key (one condition key has multiple values) fails to be replaced even if it exists in the request context.

If the condition key specified by the variable fails to be replaced, you can use its original text string as the default value. To add a default value to a variable, enclose the default value in a pair of single quotation marks (' ') and separate the condition key name from the default value with a comma and space (,). For example, if the key in **${key, 'default'}** does not exist or fails to be replaced, **${key, 'default'}** will be replaced with **default**. Condition key names are case-insensitive, but default values are case-sensitive. Spaces before and after the condition key name and the default value's single quotation marks are ignored. For example, if the principal is an IAM user, **${ g:username , 'Default_User_Name' }** will be replaced with the value of **g:UserName**. For other principals, **${ g:username , 'Default_User_Name' }** will be replaced with **Default_User_Name**.

If you want the dollar sign (**$**), which identifies a policy variable, to be interpreted literally, use **${$}**. If you want to insert a single quotation mark (') in the default value of a policy variable, use a pair of single quotation marks (''). For example, when **${g:UserName, 'A single quote is '', two quotes are ''''.'}** is replaced with the default value, it would be **A single quote is ', two quotes are ''**.

Policy variables are replaced only once. If the replacement still contains variables, they would not be replaced anymore. For example, when **${g:UserName, '${g:UserName}'}** is replaced with the default value, it would be **${g:UserName}**. The **${g:UserName}** would not be replaced again.

Policy Variable Replacement Failures

Policy variables will fail to be replaced in the following scenarios:

- The variable does not exist in the request context, for example, **"${g:UserName}"** will fail to be resolved for non-IAM user logins.
- The variable identifier is invalid, for example, **"${foo"** or **"${foo, 'default'"**.
- The default value in the variable is invalid, for example, **${key, value}**, **${foo, 'default}**, or **${foo, 'default''}**.
- The variable is empty, for example, **${}**, **${ }**, or **${ }**.
- The variable contains spaces, for example, **${g:user id}**.
- There is variable nesting, for example, **${var1${var2}}**.

Examples of Using Policy Variables

- Using variables in the Resource element
  - In the following policy, if you log in as IAM user **test_user_name** (the value of **g:UserName**), you are allowed to perform action

obs:bucket:CreateBucket on OBS bucket **OBS:*:*:bucket:test_user_name** (**"*"** is a wildcard character).

```
{
    "Version": "1.1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "obs:bucket:CreateBucket"
        ],
        "Resource": [
            "OBS:*:*:bucket:${g:UserName}"
        ]
    }]
}
```

– In the following policy, if you log in as IAM user **test_user_name** (the value of **g:UserName**), you are allowed to perform action **obs:bucket:CreateBucket** on OBS bucket **OBS:*:*:bucket:prefix_test_user_name_suffix** (**"*"** is a wildcard character).

```
{
    "Version": "1.1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "obs:bucket:CreateBucket"
        ],
        "Resource": [
            "OBS:*:*:bucket:prefix_${g:UserName}_suffix"
        ]
    }]
}
```

- Using variables in the Condition element

  In the following policy, if you log in as IAM user **test_user_name** (the value of **g:UserName**), you are allowed to perform action **iam:agencies:getAgency**.

```
{
    "Version": "1.1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:agencies:getAgency"
        ],
        "Condition": {
            "StringEquals": {
                "g:UserName": [
                    "${g:UserName}"
                ]
            }
        }
    }]
}
```

5.2 Policy Content

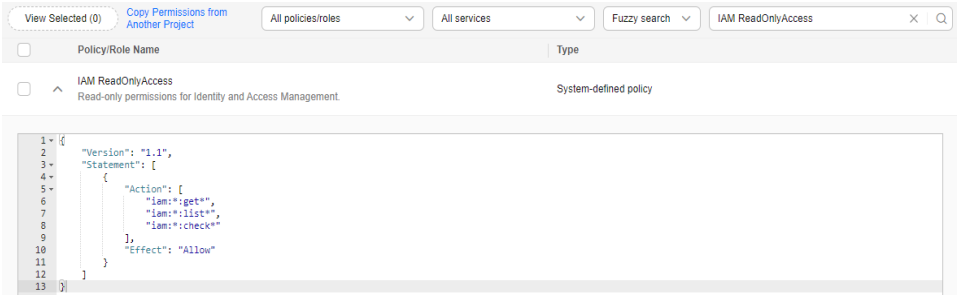
You can click a policy name to view the content of the policy.

Viewing Policy Content

Step 1 Choose **User Groups** from the left navigation pane, locate the target user group, and click **Authorize** in the **Operation** column.

Step 2 Click ⌄ on the left of a policy name to view its details. The following uses the system-defined policy **IAM ReadOnlyAccess** as an example.

Figure 5-5 Content of the IAM ReadOnlyAccess policy




```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "iam:*:get*",
            "iam:*:list*",
            "iam:*:check*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

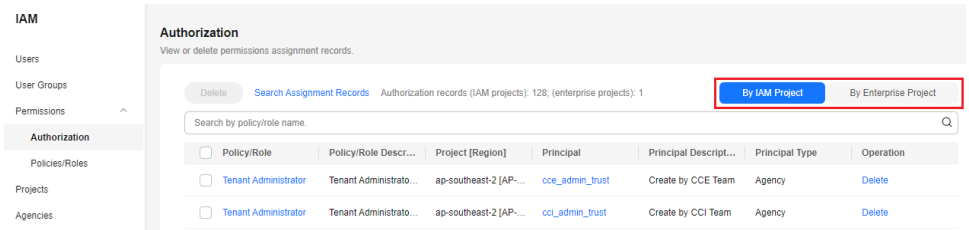
----End

5.3 Authorization Records

You can view all authorization records under your account on the **Permissions** > **Authorization** page. You can filter records by policy/role name, username, user group name, agency name, IAM project, enterprise project (if it is enabled), and principal type (user, user group, or agency).

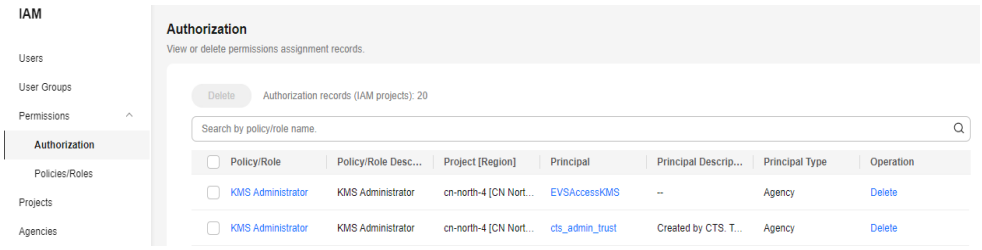
- Enterprise Project function enabled: View authorization records by IAM or enterprise project.

  Figure 5-6 Enterprise Project function enabled

- Enterprise Project function not enabled: View authorization records by IAM project. To enable Enterprise Project, see **Enabling the Enterprise Project Function**.

Figure 5-7 Enterprise Project function not enabled



Viewing Authorization Records by IAM Project

When viewing authorization records by IAM project, select the following filter conditions:

- **Policy/Role name**:

  To view the authorization records of a policy or role, select **Policy/Role name**, and enter a name. For details about the permissions of all cloud services, see **System-defined Permissions**.

- **Username/User group name/Agency name**:

  To view the IAM project permissions assigned to a specific IAM user, user group, or agency, select **Username**, **User group name**, or **Agency name**, and enter a name.

  NOTE

  For IAM project-based authorization, you assign permissions by user group. If you query the authorization records of a specific user, the authorization records of the group which the user belongs to are displayed.

- **IAM project**: The application scope of permissions. If you want to view authorization records of an IAM project, select **IAM project** and any of the following options:
  - **Global services**: View authorization records of all global services.
  - **All resources**: View authorization records of all projects, that is, the global services and all region-specific projects (including projects created later).
  - **Region-specific projects**: View authorization records of a default project or subproject (such as ap-southeast-1)
- **Principal type**: The type of objects that are authorized. There are three principal types: user, user group, and agency. In the IAM project view, you can filter records by user group or agency. If you select **User**, no records will be displayed.
- **Enterprise projects**: The name of an enterprise project. If you select **Enterprise project** and enter an enterprise project name, the **enterprise project view** is displayed.

Viewing Authorization Records by Enterprise Project

When viewing authorization records by enterprise project, select the following filter conditions:

- **Policy/Role name**:

To view the authorization records of a policy or role, select **Policy/Role name**, and enter a name. For details about the cloud service permissions supported by enterprise projects, see **Cloud Service Permissions**.

- **Username/User group name/Agency name**:

  To view the enterprise project permissions assigned to a specific IAM user or user group, select **Username** or **User group name**, and enter a name.

  NOTE

  - For enterprise project-based authorization, you assign permissions by user. If you query the authorization records of a specific user, the authorization records of the user and the user group which the user belongs to are displayed.

- **Enterprise project**: The name of an enterprise project, that is, the application scope of permissions. To view the authorization records of a specific enterprise project, select **Enterprise project**, and enter an enterprise project name.
- **Principal type**: The type of objects that are authorized. There are three principal types: user, user group, and agency.
- **IAM project**: The name of an IAM project or region. If you select **IAM project** and enter a project name, the **IAM project view** is displayed.

5.4 Custom Policies

5.4.1 Creating a Custom Policy

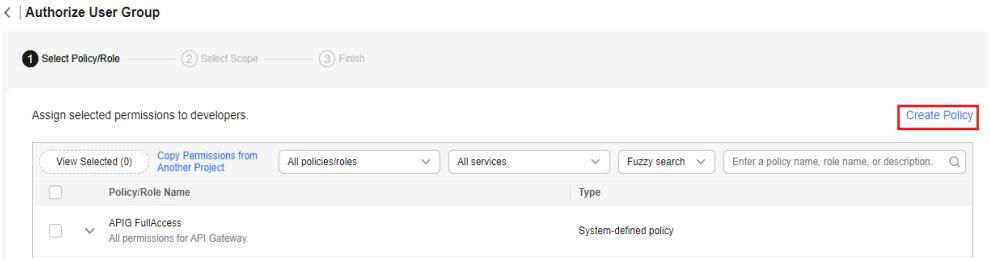
You can create custom policies to supplement system-defined policies and implement more refined access control.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of JSON syntax.
- JSON: Create a JSON policy or edit an existing one.

This section describes how to create custom policies on the **Permissions** > **Policies/Roles** page. You can also create custom policies during authorization (see **Figure 5-8**).

Figure 5-8 Creating a policy during authorization

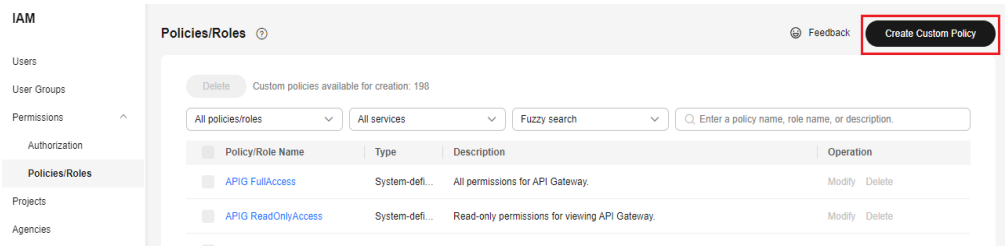


Creating a Custom Policy in the Visual Editor

Step 1 Log in to the **IAM console**.

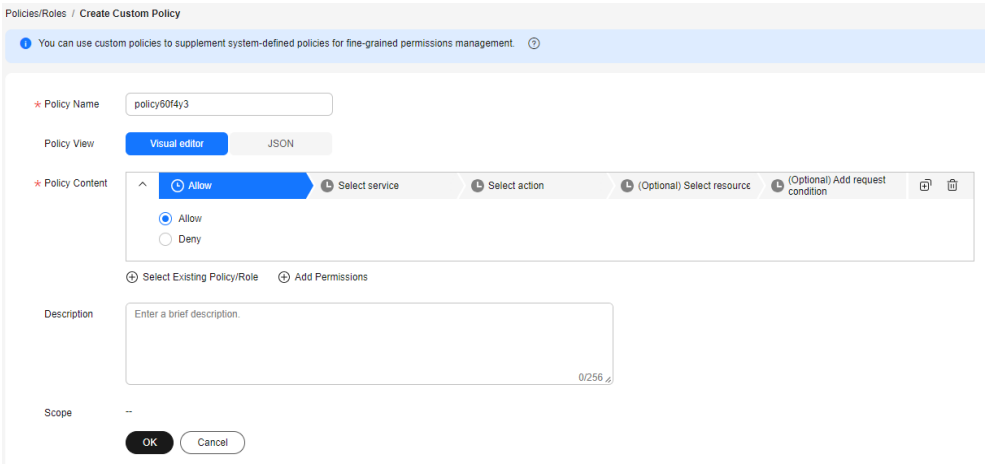
Step 2 On the IAM console, choose **Permissions** > **Policies/Roles** from the navigation pane, and click **Create Custom Policy** in the upper right corner.

Figure 5-9 Creating a custom policy



Step 3 Enter a policy name.

Figure 5-10 Entering a policy name



Step 4 Select **Visual editor** for **Policy View**.

Step 5 Set the policy content.

1. Select **Allow** or **Deny**.
2. Select a cloud service.

   NOTE

   - Only one cloud service can be selected for each permission block. To configure permissions for multiple cloud services, click **Add Permissions**, or switch to the JSON view (see **Creating a Custom Policy in JSON View**).
   - A custom policy can contain permissions for either global or project-level services. To define permissions required to access both global and project-level services, enclose the permissions in two separate custom policies for refined authorization.
3. Select actions.
4. (Optional) Select all resources, or select specific resources by specifying their paths.

   For details about cloud services that support resource-level authorization, see **Cloud Services that Support Resource-Level Authorization Using IAM**.

Table 5-11 Resource type

Parameter	Description
Specific	Permissions for specific resources. For example, to define permissions for buckets whose names start with **TestBucket**, specify the bucket resource path as **OBS:*:*:bucket:TestBucket***. **NOTE** – Specifying bucket resources Format: "OBS:*:*:bucket:*Bucket name*". For bucket resources, IAM automatically generates the prefix of the resource path: **obs:*:*:bucket:**. For the path of a specific bucket, add the *bucket name* to the end. You can also use a wildcard character (*) to indicate any bucket. For example, **obs:*:*:bucket:*** indicates any OBS bucket. – Specifying object resources Format: "OBS:*:*:object:*Bucket name/object name*". For object resources, IAM automatically generates the prefix of the resource path: **obs:*:*:object:**. For the path of a specific object, add the *bucket name/object name* to the end of the resource path. You can also use a wildcard character (*) to indicate any object in a bucket. For example, **obs:*:*:object:my-bucket/my-object/*** indicates any object in the **my-object** directory of the **my-bucket** bucket.
All	Permissions for all resources.

5. (Optional) Add request conditions by specifying condition keys, operators, and values.

Table 5-12 Condition parameters

Name	Description
Condition Key	A key in the Condition element of a statement. There are global and service-specific condition keys. **Global condition keys** (starting with **g:**) are available for operations of all services, whereas service-specific condition keys (starting with a service abbreviation name such as **obs:**) are available only for operations of the corresponding service. For details, see the user guide of the corresponding cloud service, for example, see **OBS Request Conditions**. Condition keys are case insensitive.
Operator	Used together with a condition key and condition value to form a complete condition statement.
Value	Used together with a condition key and an operator that requires a keyword, to form a complete condition statement.

Figure 5-11 Adding a request condition

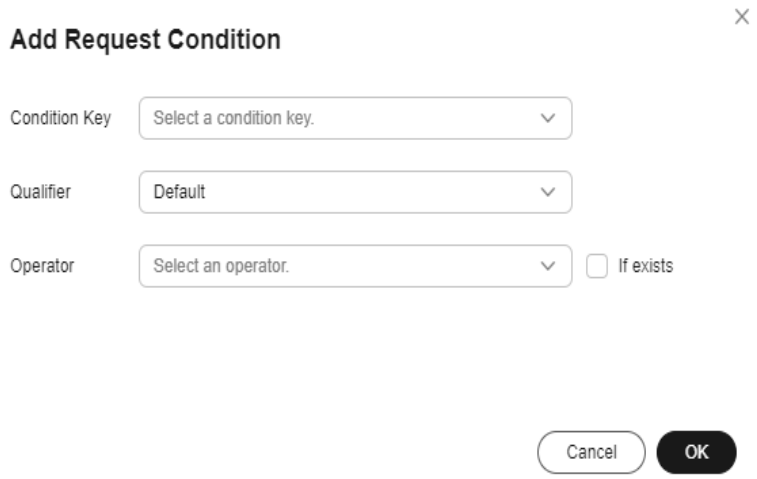


Table 5-13 Global condition keys

Global Condition Key	Type	Description
g:CurrentTime	Time	Time when an authentication request is received. The time is in ISO 8601 format, for example, **2012-11-11T23:59:59Z**.
g:DomainName	String	Account name.
g:MFAPresent	Boolean	Whether to obtain a token through MFA authentication.
g:MFAAge	Number	Validity period of a token obtained through MFA authentication. This condition must be used together with **g:MFAPresent**.
g:ProjectName	String	Project name.
g:UserId	String	IAM user ID.
g:UserName	String	IAM username.

Step 6 (Optional) Switch to the JSON view and modify the policy content in JSON format.

NOTE

If the modified policy content is incorrect, check and modify the content again, or click **Reset** to cancel the modifications.

Step 7 (Optional) To add another permission block for the policy, click **Add Permissions**. Alternatively, click the plus (+) icon on the right of an existing permission block to clone its permissions.

Step 8 (Optional) Enter a brief description for the policy.

Step 9 Click **OK**.

Step 10 Attach the policy to a user group. Users in the group then inherit the permissions defined in this policy.

NOTE

You can attach custom policies to a user group in the same way as you attach system-defined policies. For details, see **Creating a User Group and Assigning Permissions**.

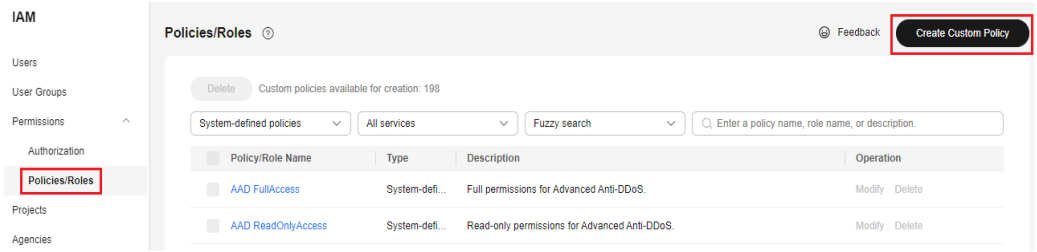
----End

Creating a Custom Policy in JSON View

Step 1 Log in to the **IAM console**.

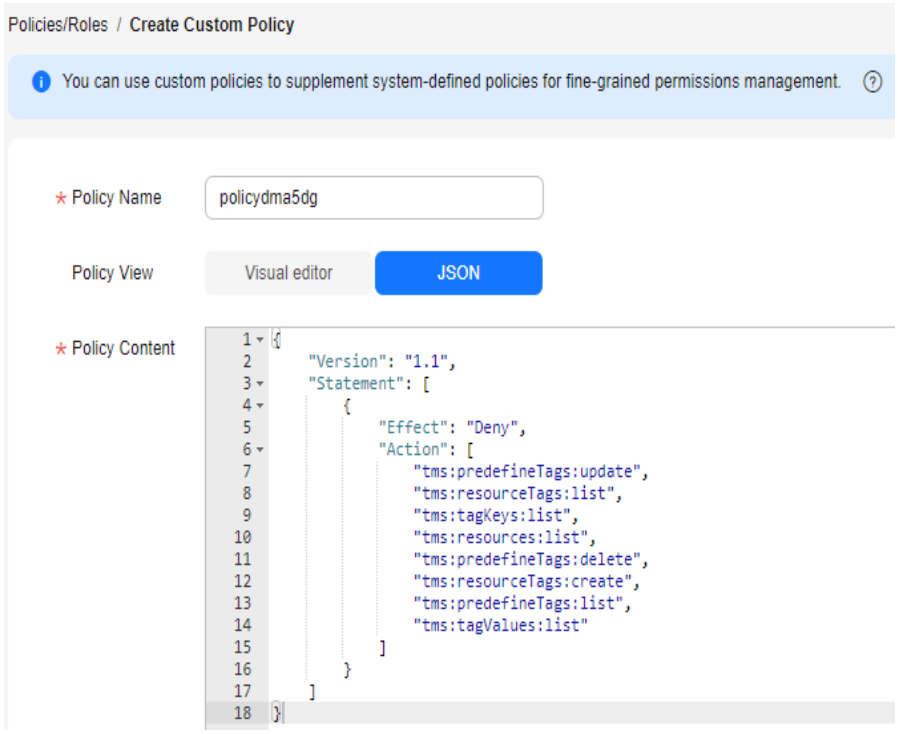
Step 2 On the IAM console, choose **Permissions** > **Policies/Roles** from the navigation pane, and click **Create Custom Policy** in the upper right corner.

Figure 5-12 Creating a custom policy



Step 3 Enter a policy name.

Figure 5-13 Entering a policy name



Step 4 Select **JSON** for **Policy View**.

Step 5 (Optional) Click **Select Existing Policy/Role** and select a policy/role to use it as a template, for example, select **EVS FullAccess**.

NOTE

If you select multiple policies, all of them must have the same scope, that is, either **Global services** or **Project-level services**. To define permissions required to access both global and project-level services, enclose the permissions in two separate custom policies for refined authorization.

Step 6 Click **OK**.

Step 7 Modify the statement in the template.

- **Effect**: Set it to **Allow** or **Deny**.
- **Action**: Enter the actions listed in the API actions table (see **Figure 5-14**) of the EVS service, for example, **evs:volumes:create**.

Figure 5-14 API actions

Permission	API	Action
Listing IAM Users	GET /v3/users	iam:users:listUsers

NOTE

- The version of each custom policy is fixed at **1.1**.
- For details about the API actions supported by each service, see **System-defined Permissions**.

Step 8 (Optional) Enter a brief description for the policy.

Step 9 Click **OK**. If the policy list is displayed, the policy is created successfully. If a message indicating incorrect policy content is displayed, modify the policy.

Step 10 Attach the policy to a user group. Users in the group then inherit the permissions defined in this policy.

NOTE

You can attach custom policies to a user group in the same way as you attach system-defined policies. For details, see **Creating a User Group and Assigning Permissions**.

----End

5.4.2 Modifying or Deleting a Custom Policy

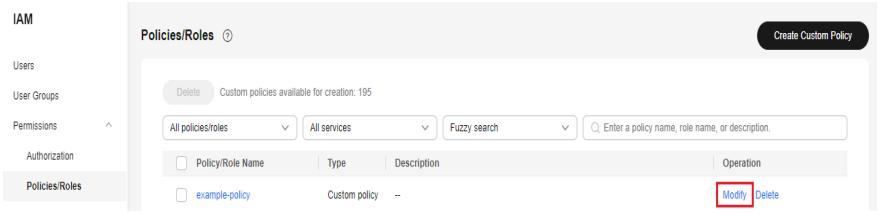
You can modify or delete custom policies as needed.

Modifying a Custom Policy

Modify the name, description, or content of a custom policy.

1. In the left navigation pane on the **IAM console**, choose **Permissions** > **Policies/Roles**.
2. Locate the custom policy you want to modify and click **Modify** in the **Operation** column, or click the custom policy name to go to the policy details page.

Figure 5-15 Modifying a custom policy



3. Modify the name or description of the policy as required.
4. Modify the policy content by following the instructions provided in **Creating a Custom Policy in the Visual Editor** as required.
5. Click **OK** to save the modifications.

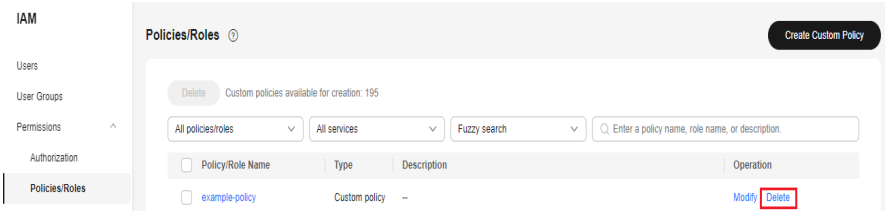
Deleting a Custom Policy

NOTE

Only custom policies that are not attached to any user groups or agencies can be deleted. If a custom policy has been attached to certain user groups or agencies, detach the policy and then delete it.

1. In the left navigation pane on the **IAM console**, choose **Permissions** > **Policies/Roles**.
2. In the row containing the custom policy you want to delete, click **Delete**.

Figure 5-16 Deleting a custom policy



3. Click **OK**.

5.4.3 Custom Policy Examples

Using a Custom Policy Along with Full-Permission System-Defined Policies

If you want to assign full permissions to a user but disallow them from accessing a specific service, such as Cloud Trace Service (CTS), create a custom policy for denying access to CTS and then attach this custom policy together with the **FullAccess** policy to the user. As an explicit deny in any policy overrides any allows, the user can perform operations on all services except CTS.

Example policy denying access only to CTS:


```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
               "cts:*:*"
         ]
      }
   ]
}
```

NOTE

- **Action**: Operations to be performed. Each action must be defined in the format "*Service name*:*Resource type*:*Operation*".

  For example, **cts:*:*** refers to permissions for performing all operations on all resource types of CTS.
- **Effect**: Determines whether to deny or allow the operation.

Using a Custom Policy Along with a System-Defined Policy

- If you want to assign full permissions to a user but disallow them from creating BMSs, create a custom policy denying the **bms:servers:create** action and then attach this custom policy together with the **BMS FullAccess** policy to the user. As an explicit deny in any policy overrides any allows, the user can perform all operations on BMS except creating BMSs.

  Example policy denying BMS creation:

  ```
  {
     "Version": "1.1",
     "Statement": [
        {
           "Effect": "Deny",
           "Action": [
                 "bms:servers:create"
           ]
        }
     ]
  }
  ```

- If you want to assign OBS read-only permissions to all users but disallow certain users from viewing specific resources, for example, disallow users whose names start with **TestUser** from viewing buckets whose names start with **TestBucket**, create a custom policy denying such operations and attach this custom policy together with the OBS ReadOnlyAccess policy to those users. As an explicit deny in any policy overrides any allows, certain users cannot view buckets whose names start with **TestBucket**.

  Example policy denying users whose names start with **TestUser** from viewing buckets whose names start with **TestBucket**:

  ```
  {
        "Version": "1.1",
        "Statement": [
              {
                    "Effect": "Deny",
                    "Action": [
                          "obs:bucket:ListAllMybuckets",
                          "obs:bucket:HeadBucket",
                          "obs:bucket:ListBucket",
                          "obs:bucket:GetBucketLocation"
                    ],
                    "Resource": [
                       "obs:*:*:bucket:TestBucket*"
  ```



```
                ],
                "Condition": {
                    "StringStartWith": {
                        "g:UserName": [
                            "TestUser"
                ]
                    }
                }
                }
        ]
}
```

NOTE

Currently, only certain cloud services (such as OBS) support resource-based authorization. For services that do not support this function, you cannot create custom policies containing resource types.

Using Only a Custom Policy

You can create a custom policy and attach only the custom policy to the group which the user belongs to.

- The following is an example policy that allows access only to ECS, EVS, VPC, ELB, and Application Operations Management (AOM).

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow"
            "Action": [
                "ecs:*:*",
                "evs:*:*",
                "vpc:*:*",
                "elb:*:*",
                "aom:*:*"
            ]
        }
    ]
}
```

- The following is an example policy that allows only IAM users whose names start with **TestUser** to delete all objects in the **my-object** directory of the bucket **my-bucket**.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:DeleteObject"
            ],
            "Resource": [
                "obs:*:*:object:my-bucket/my-object/*"
            ],
            "Condition": {
                "StringStartWith": {
                    "g:UserName": [
                        "TestUser"
                ]
            }
        }
    ]
}
```

- The following is an example policy that allows access to all services except ECS, EVS, VPC, ELB, AOM, and APM.


```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "*:*:*"
            ]
        },
        {
            "Action": [
                "ecs:*:*",
        "evs:*:*",
        "vpc:*:*",
        "elb:*:*",
        "aom:*:*",
        "apm:*:*"
            ],
            "Effect": "Deny"
        }
    ]
}
```

5.4.4 Cloud Services that Support Resource-Level Authorization Using IAM

If you want to grant permissions to an IAM user for specific resources, **create a custom policy** that contains permissions for the resources, and attach the policy to the user. The user then only has the permissions for the specified resources. For example, to grant permissions to an IAM user for buckets whose names start with **TestBucket**, create a custom policy, specify the resource path as **OBS:*:*:bucket:TestBucket***, and attach the policy to the user.

The following table lists the cloud services that support resource-level authorization and the supported resource types.

Table 5-14 Cloud services that support resource-level authorization and the supported resource types

Service	Resource Type	Resource Name
Open API platform SaaS (Apiexplorer-saas)	product	Product
	portal	Portal
Cloud Bastion Host (CBH)	instanceId	Instance ID
Cloud Container Engine (CCE)	cluster	Cluster
Cloud Operations Center (COC)	schedule	Scheduled O&M
	document	Document
	drillPlan	Drill plan
	attackTask	Attack task
	contingencyPlan	Contingency plan

Service	Resource Type	Resource Name
	drillTask	Drill task
	accountBaseline	Account baseline
	faultMode	Fault mode
	drillRecord	Drill record
	job	Task
	slaTemplate	SLA template
	attackTargetRecord	Attack target record of an attack task
	parameter	Configuration parameter
Cloud Secret Management Service (CSMS)	secretName	Secret name
DataArts Insight	workspace	Workspace
Distributed Cache Service (DCS)	instance	Instance
Document Database Service (DDS)	instanceName	Instance name
Data Lake Insight (DLI)	queue	DLI queue
	database	DLI database
	table	DLI table
	column	DLI column
	datasourceauth	DLI security authentication information
	jobs	DLI job
	resource	Resource package
	elasticresourcepool	Elastic resource pool
	group	Resource package group
	variable	Global variable
Distributed Message Service (DMS)	**rabbitmq**	RabbitMQ instance
	kafka	Kafka instance
	rocketmq	RocketMQ instance
GaussDB(DWS)	cluster	Cluster

Service	Resource Type	Resource Name
Elastic Cloud Server (ECS)	instance	ECS
Elastic Volume Service (EVS)	volume	EVS disk
FunctionGraph	function	Function
	trigger	Trigger
Graph Engine Service (GES)	graphName	GES graph name
	backupName	GES backup name
	metadataName	Metadata name
Intelligent EdgeFabric (IEF)	product	Product
	node	Edge node
	group	Edge node group
	deployment	Deployment
	batchjob	Batch job
	application	Application template
	appVersion	Application template version
	IEFInstance	IEF instance
Data Encryption Workshop (DEW)	KeyId	Key ID
MapReduce Service (MRS)	cluster	Cluster
Object Storage Service (OBS)	bucket	Bucket
	object	Object
Relational Database Service (RDS)	instance	RDS instance
Resource Formation Service (RFS)	privateModule	Private module
	stack	Stack
	stackSet	Stack set
	privateTemplate	Private template
	privateProvider	Private provider
ROMA Connect	graph	Business flow diagram ID

Service	Resource Type	Resource Name
SSL Certificate Manager (SCM)	cert	Certificate ID
SecMaster	alert	Alarm
	search	Query
	playbook	Playbook
	workflow	Workflow
	subscription	Subscription
	indicator	Threat intelligence
	alertRule	Alert model
	connection	Asset connection
	mapping	Categorical mapping
	dataclass	Data class
	report	Report
	searchCondition	Retrieval criteria
	agency	Agency
	resource	Resource
	layout	Layout
	dataobject	Data object
	emergencyVulnerability	Emergency vulnerability
	workspace	Workspace
	metric	Metric
	dataspace	Data space
	catalogue	Directory
	task	To-do task
	alertRuleTemplate	Alarm template
	pipe	Data pipeline
	incident	Incident
	table	Table
	vulnerability	Vulnerability
Software Repository for Container (SWR)	chart	Chart

Service	Resource Type	Resource Name
	repository	Repository
	instance	Enterprise edition instance
Virtual Private Cloud (VPC)	publicip	EIP

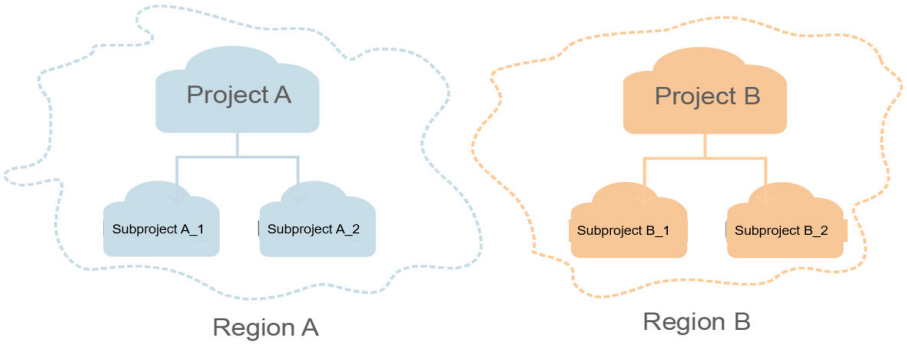
6 Project Management

Projects are used to isolate resources (including compute, storage, and network resources) among physical regions. A project is provided for each region by default, and permissions are assigned based on projects. Preset projects cannot be deleted.

For more refined access control, create subprojects under a project and purchase resources in the subprojects. Then, provide users with permissions to access resources in specific subprojects.

IAM projects are different from enterprise projects. For details about their differences, see **What Are the Differences Between IAM Projects and Enterprise Projects?**

Figure 6-1 Project isolation



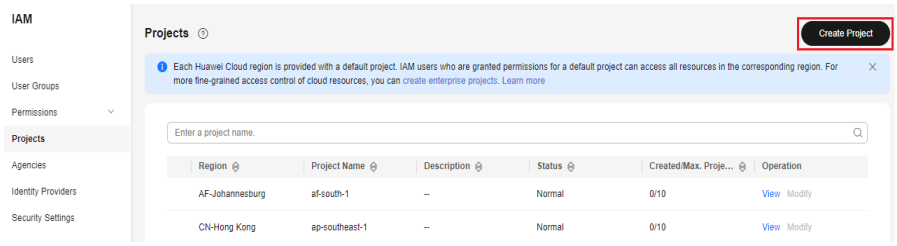
NOTE

- Resources cannot be transferred across IAM projects.
- You cannot create projects in IAM after enabling the Enterprise Project function.

Creating a Project

Step 1 In the left navigation pane on the **IAM console**, choose Projects and click **Create Project**.

Figure 6-2 Creating a project



Step 2 Select a region in which you want to create a subproject.

Step 3 Enter a project name.

NOTE

- The project name will be in the format "*Name of the default project for the selected region_Custom project name*". The name of default projects cannot be modified.
- The project name can only contain letters, digits, hyphens (-), and underscores (_). The total length of the project name cannot exceed 64 characters.

Step 4 (Optional) Enter a description for the project.

Step 5 Click **OK**.

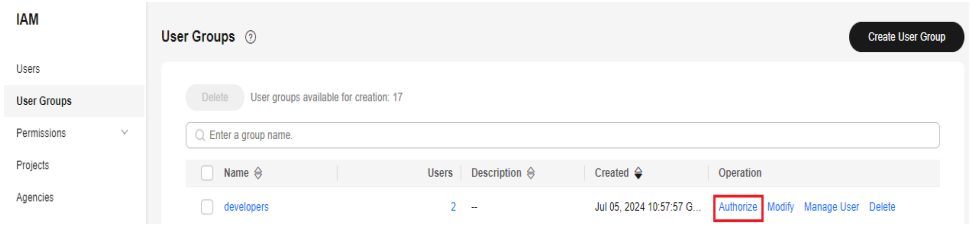
----End

Granting a User Group Permissions for a Project

You can assign permissions based on projects to control access to resources in specific projects.

Step 1 In the user group list, click **Authorize** in the row containing the target user group.

Figure 6-3 Managing permissions



Step 2 On the **Authorize User Group** page, select the policies or roles to be attached to the user group and click **Next**.

Step 3 Specify the authorization scope. If you select **Region-specific projects**, select one or more projects.

Step 4 Click **OK**.

NOTE

For more information about user group authorization, see **Creating a User Group and Assigning Permissions**.

----End

Switching Regions or Projects

For project-level services, switch to a region or project in which you have been authorized to access cloud services. You do not need to switch regions or projects for global services.

Step 1 Log in to the Huawei Cloud management console.

Step 2 Go to a project-level cloud service page. Click the drop-down list box in the upper left corner of the page and select a region.

----End

7 Agency Management

7.1 Agency Overview

Introduction

A trust agency is a trust relationship established between you and other companies, Huawei Cloud accounts or cloud services. If you have purchased different types of resources on Huawei Cloud, you can create a trust agency on IAM to entrust a professional company, account, or cloud service to perform secure, efficient O&M on your behalf. The entrusted account, company, or cloud service can perform resource O&M on your behalf based on assigned permissions.

Agency Type

- Account Agency: An account agency enables you to delegate another account to implement O&M on your resources based on assigned permissions.
- Service Agency: Huawei Cloud services interwork with each other, and some cloud services are dependent on other services. To delegate a cloud service to access other services and perform resource O&M, create a service agency for the service.

Advantages

- Flexible management: You can grant permissions to an account agency or a cloud service agency, and delegate some services to professional companies.
- Security and reliability: The delegated party can only use resources based on the permissions granted, ensuring the security of accounts, data, and resources. The delegating party can create, modify, or cancel a delegation at any time to flexibly control resource access.

7.2 Delegating Another Account for Resource Management

7.2.1 Process for Account Delegation

The agency function enables you to delegate another account to implement O&M on your resources based on assigned permissions.

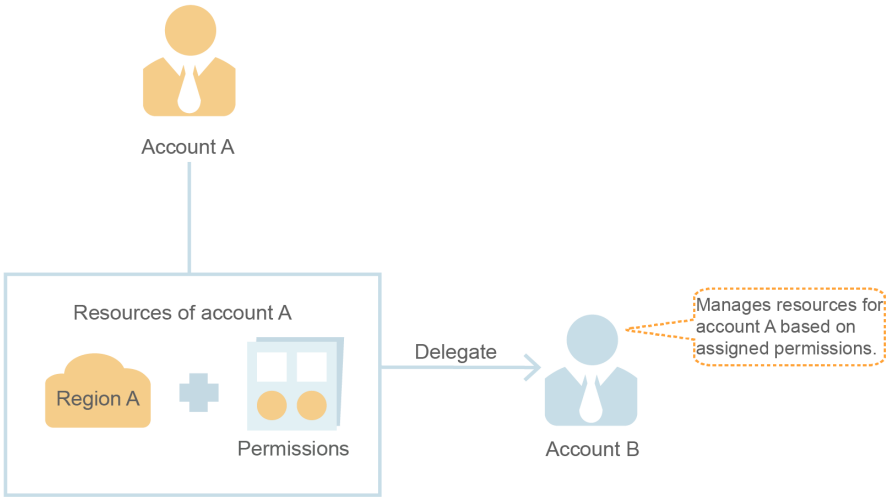
NOTE

You can delegate resource access only to accounts, rather than IAM users.

The following is the procedure for delegating resource access to another account. Account A is the delegating party and account B is the delegated party.

Step 1 Account A creates an agency in IAM to delegate resource access to account B.

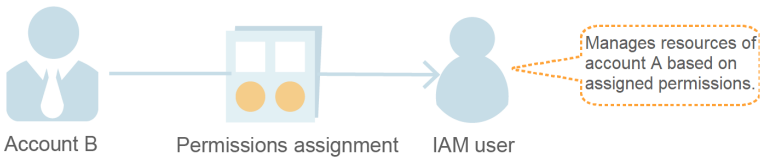
Figure 7-1 (Account A) Creating an agency



Step 2 (Optional) Account B assigns permissions to an IAM user to manage specific resources for account A.

1. Create a user group, and grant it permissions required to manage account A's resources.
2. Create a user and add the user to the user group.

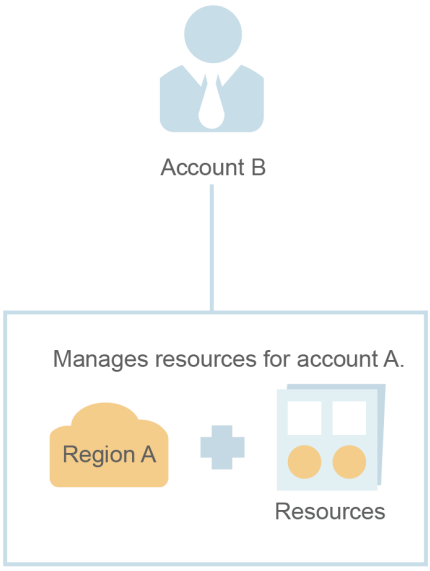
Figure 7-2 (Account B) Authorizing an IAM user to manage delegated resources



Step 3 Account B or the authorized user manages account A's resources.

1. Use account B to log in and switch the role to account A.
2. Switch to region A and manage account A's resources in this region.

Figure 7-3 (Account B) Switching the role



----End

7.2.2 Creating an Agency and Assigning Permissions

By creating an agency, you can share your resources with another account, or delegate an individual or team to manage your resources. You do not need to share your security credentials (the password or access keys) with the delegated party. Instead, the delegated party can log in with its own account credentials and then switches the role to your account and manage your resources.

Prerequisites

Before creating an agency, complete the following operations:

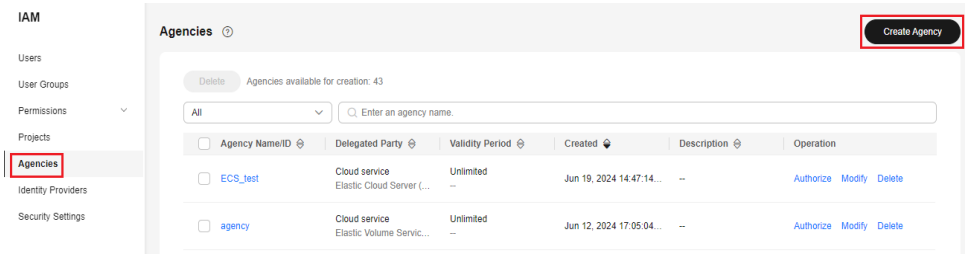
- Understand the **basic concepts** of permissions.
- Determine the **system-defined permissions** to be assigned to the agency, and check whether the permissions have dependencies. If yes, assign dependent permissions by referring to **Assigning Dependency Roles**.

Procedure

Step 1 Log in to the **IAM console**.

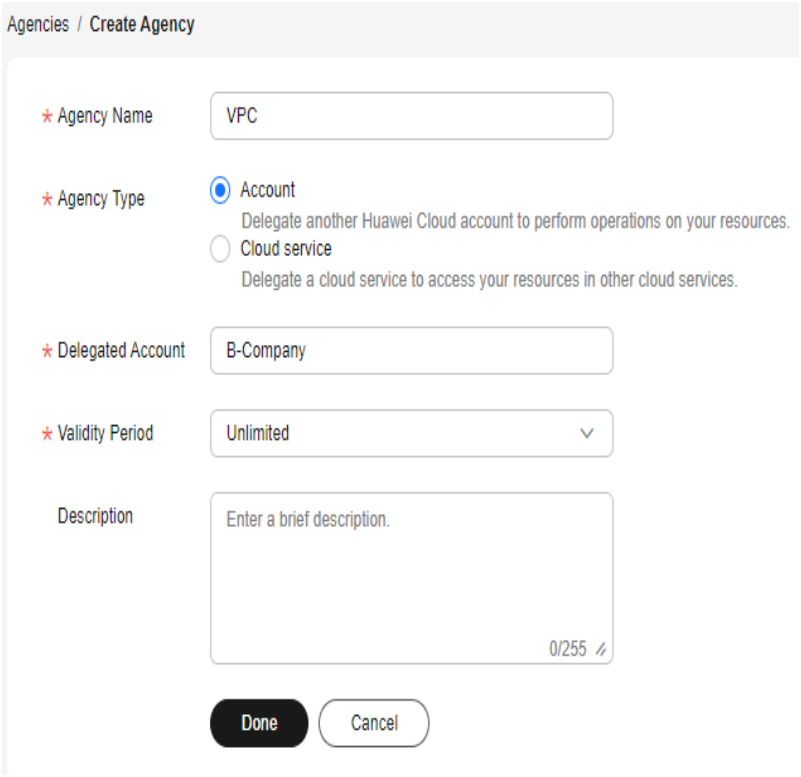
Step 2 On the IAM console, choose **Agencies** from the left navigation pane, and click **Create Agency** in the upper right corner.

Figure 7-4 Creating an agency



Step 3 Enter an agency name.

Figure 7-5 Setting the agency name



Step 4 Specify the agency type as **Account**, and enter the name of a delegated account.

NOTE

- **Account**: Share resources with another account or delegate an individual or team to manage your resources. The delegated account can only be an account, rather than an IAM user or a federated user.
- **Cloud service**: Delegate a specific service to access other services. For more information, see **Delegating Another Service for Resource Management**.

Step 5 Set the validity period and enter a description for the agency.

Step 6 Click **Done**.

If you do not need to authorize the agency, click **Cancel** to return to the agency list and view the created agency. In this case, the created agency does not have any permissions.

Step 7 In the displayed dialog box, click **Authorize**.

Step 8 Select the policies or roles to be attached to the agency, click **Next**, and select the authorization scope.

NOTE

- Assigning permissions to an agency is similar to assigning permissions to a user group. The two operations differ only in the number of available permissions. For details about how to assign permissions to a user group, see **Assigning Permissions to a User Group**.
- You can assign the **Security Administrator** role to the agency, but we do not recommend you to do so. For account security purposes, only grant the required permissions to the agency based on the principle of least privilege (PoLP).

Step 9 Click **OK**.

NOTE

After creating an agency, provide your account name, agency name, agency ID, and agency permissions to the delegated party. The delegated party can then switch the role to your account and manage specific resources based on the assigned permissions.

----End

7.2.3 Assigning Agency Permissions to an IAM User

When a trust relationship is established between your account and another account, you become a delegated party. By default, only your account and the members of the **admin** group can manage resources for the delegating party. To authorize IAM users to manage these resources, assign permissions to the users.

You can authorize an IAM user to manage resources for all delegating parties, or authorize the user to manage resources for a specific delegating party.

Prerequisites

- A trust relationship has been established between your account and another account.
- You have obtained the name of the delegating account and the name and ID of the created agency.

Procedure

Step 1 Create a user group and grant permissions to it.

1. On the **User Groups** page, click **Create User Group**.
2. Enter a user group name.
3. Click **OK**.
4. In the row containing the user group, click **Authorize**.
5. Create a custom policy.

   NOTE

   This step is used to create a policy containing permissions required to manage resources for a specific agency. If you want to authorize an IAM user to manage resources for all agencies, go to step **Step 1.6**.

   a. On the **Select Policy/Role** page, click **Create Policy** in the upper right corner of the permission list.

   b. Enter a policy name.

c. Select **JSON** for **Policy View**.

d. In the **Policy Content** area, enter the following content:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "iam:tokens:assume"
            ],
            "Resource": {
                "uri": [
                    "/iam/agencies/agencyTest"
                ]
            },
            "Effect": "Allow"
        }
    ]
}
```

NOTE

- Replace **agencyTest** with the agency name obtained from a delegating party. Copy the other content without making any changes.
- For more information about permissions, see **Permissions Management**.

e. Click **Next**.

6. Select the policy created in the previous step or the **Agent Operator** role and click **Next**.
   - Custom policy: Allows a user to manage resources only for an agency identified by a specific ID.
   - **Agent Operator** role: Allows a user to manage resources for all agencies.
7. Specify the authorization scope.
8. Click **OK**.

Step 2 Create an IAM user and add the user to the user group.

1. On the **Users** page, click **Create User**.
2. On the **Create User** page, enter a username.
3. Select **Management console access** for **Access Type** and then select **Set by user** for **Credential Type**.
4. Enable login protection and click **Next**.
5. Select the user group created in step **Step 1** and click **Create**.

NOTE

After the authorization is complete, the IAM user can switch to the account of the delegating party and manage specific resources under the account.

----End

Related Operations

The delegated account or the authorized IAM users can **switch their roles** to the delegating account to view and use its resources.

7.2.4 Managing Delegated Resources

When an account establishes a trust relationship with your account, you become a delegated party. The IAM users granted agency permissions can switch to the delegating accountand manage resources under the account based on the granted permissions.

Prerequisites

- A trust relationship has been established between your account and another account.
- You have obtained the delegating account name and agency name.

Procedure

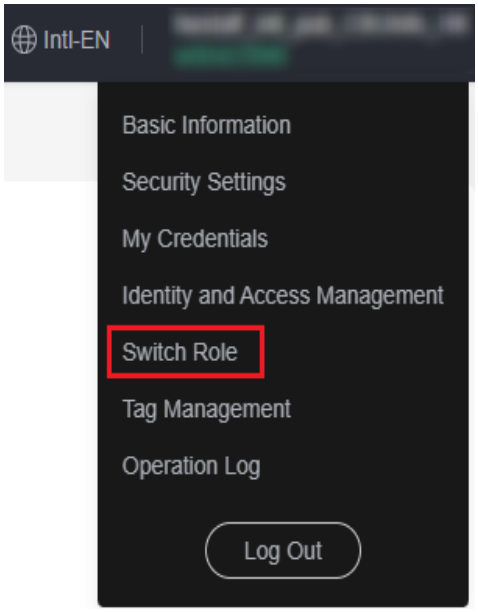
Step 1 Log in to the Huawei Cloud console using your account, or log in as the IAM user created in "Assigning Permissions to an IAM User (by a Delegated Party)".

NOTE

The IAM user created in "Assigning Permissions to an IAM User (by a Delegated Party)" has permission to manage agencies and switch roles.

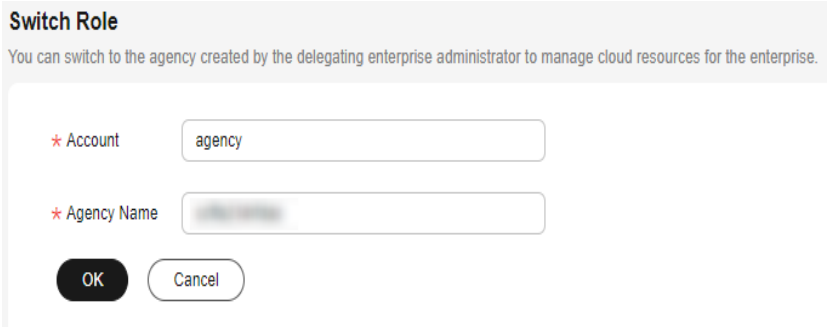
Step 2 Hover the mouse pointer over the username in the upper right corner and choose **Switch Role**.

Figure 7-6 Switching the role



Step 3 On the **Switch Role** page, enter the account name of the delegating party.

Figure 7-7 Entering the account name and agency name of the delegating party



NOTE

After you enter the account name, the agencies created under this account will be automatically displayed after you click the agency name text box. Select an authorized one from the drop-down list.

Step 4 Click **OK** to switch to the delegating account.

----End

Follow-Up Procedure

To return to your own account, hover the mouse pointer over the username in the upper right corner, choose **Switch Role**, and select your account.

7.3 Delegating Another Service for Resource Management

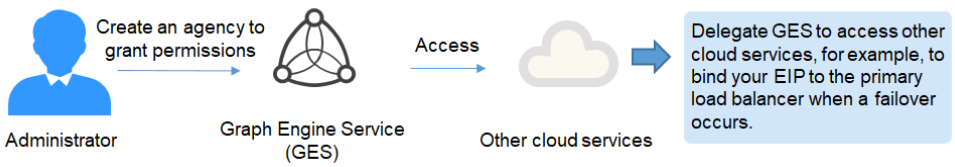
Huawei Cloud services interwork with each other, and some cloud services are dependent on other services. To delegate a cloud service to access other services and perform resource O&M, create an agency for the service.

IAM provides two methods to create a cloud service agency:

1. **Creating a cloud service agency on the IAM console**

   For example, create an agency for Graph Engine Service (GES) and grant it permissions to bind your EIP to the primary load balancer if a failover occurs.

   Figure 7-8 Cloud service agency

2. Automatically creating a cloud service agency to use certain resources

   The following takes Scalable File Service (SFS) as an example to describe the procedure for automatically creating a cloud service agency:

a. Go to the SFS console.
b. On the **Create File System** page, enable static data encryption.
c. A dialog box is displayed requesting you to confirm the creation of an SFS agency. After you click **OK**, the system automatically creates an SFS agency with **KMS CMKFullAccess** permissions for the current project. With the agency, SFS can obtain KMS keys for encrypting or decrypting file systems.
d. You can view the agency in the agency list on the IAM console.

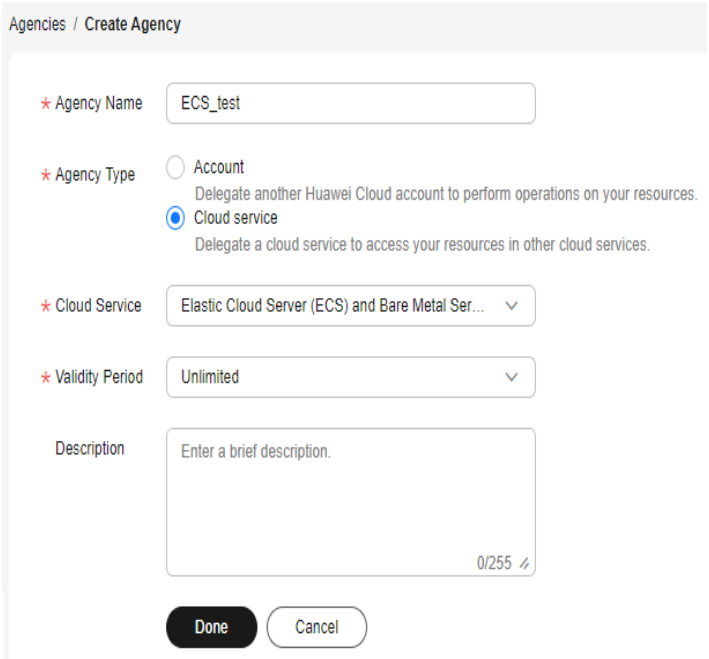
Creating a Cloud Service Agency on the IAM Console

Step 1 Log in to the **IAM console**.

Step 2 On the IAM console, choose **Agencies** from the navigation pane, and click **Create Agency**.

Step 3 Enter an agency name.

Figure 7-9 Cloud service agency name



Step 4 Select the **Cloud service** agency type, and then select a service.

Step 5 Select a validity period.

Step 6 (Optional) Enter a description for the agency to facilitate identification.

Step 7 Click **Done**.

If you do not need to authorize the agency, click **Cancel** to return to the agency list and view the created agency. In this case, the created agency does not have any permissions.

Step 8 In the displayed dialog box, click **Authorize**.

Step 9 Select the permissions to be assigned to the agency, click **Next**, and specify the authorization scope.

Step 10 Click **OK**.

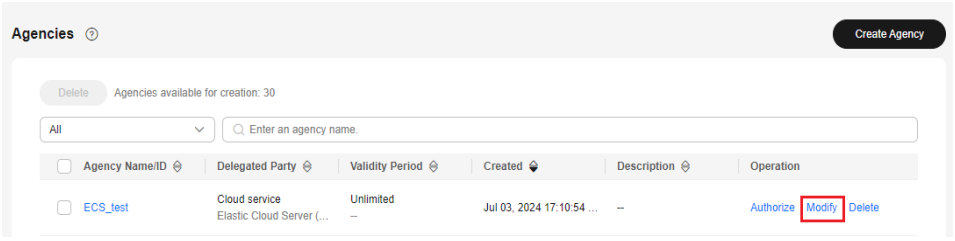
----End

7.4 Deleting or Modifying Agencies

Modifying an Agency

To modify the permissions, validity period, and description of an agency, click **Modify** in the row containing the agency you want to modify.

Figure 7-10 Modifying an agency



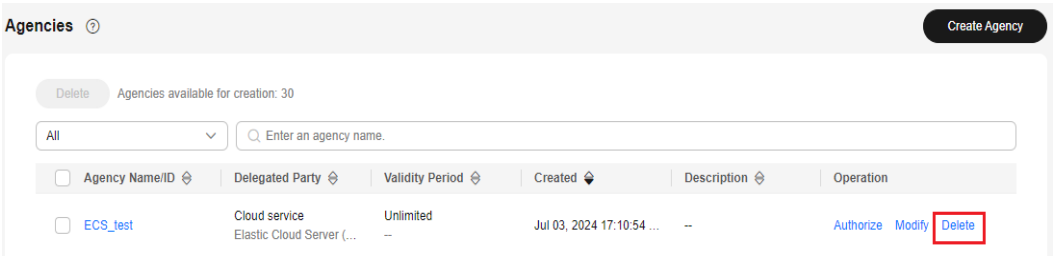
NOTE

- You can change the cloud service, validity period, description, and permissions of cloud service agencies, but you cannot change the agency name and type.
- Modifying the permissions of cloud service agencies may affect the usage of certain functions of cloud services. Exercise caution when performing this operation.

Deleting an Agency

To delete an agency, click **Delete** in the row containing the agency to be deleted and click **OK**.

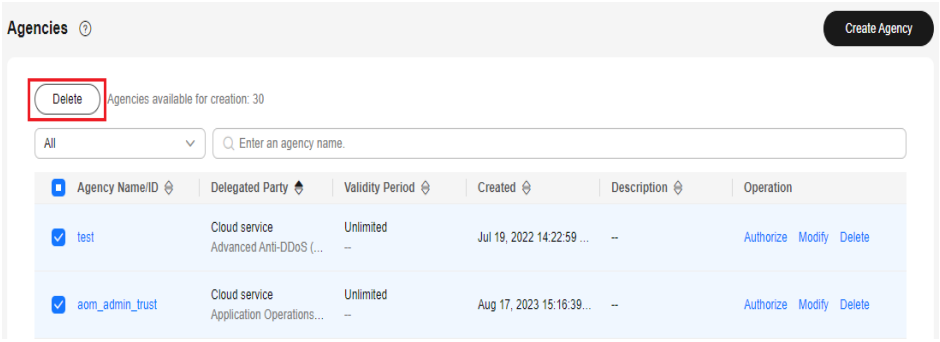
Figure 7-11 Deleting an agency



Batch Deleting Agencies

To delete multiple agencies, select the agencies to be deleted in the list and click **Delete** above the list.

Figure 7-12 Batch deleting agencies



NOTE

After you delete an agency, all permissions granted to the delegated accounts will be revoked.

8 Security Settings

8.1 Security Settings Overview

You can configure the account settings, critical operation protection, login authentication policy, password policy, and access control list (ACL) on the **Security Settings** page. For details, see **Basic Information**, **Critical Operation Protection**, **Login Authentication Policy**, **Password Policy**, and **ACL**. This chapter describes how to access the **Security Settings** page and who is the intended audience.

Intended Audience

Table 8-1 lists the intended audience of different functions provided on the **Security Settings** page and their access permissions for the functions.

Table 8-1 Intended audience

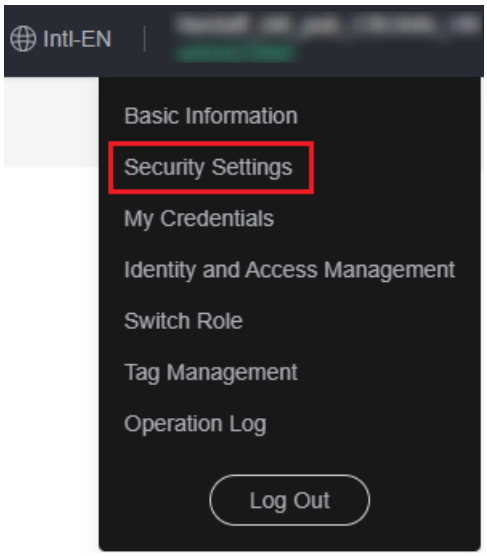
Function	Intended Audience
Basic Information	• IAM users: Full access • Account: To change the basic information, see **Basic Information Management**.
Critical Operations	• **Administrator**: Full access • IAM users: Read-only access
Login Authentication Policy	• **Administrator**: Full access • IAM users: Read-only access
Password Policy	• **Administrator**: Full access • IAM users: Read-only access

Function	Intended Audience
ACL	• Administrator: Full access • IAM users: Read-only access

Accessing the Security Settings Page

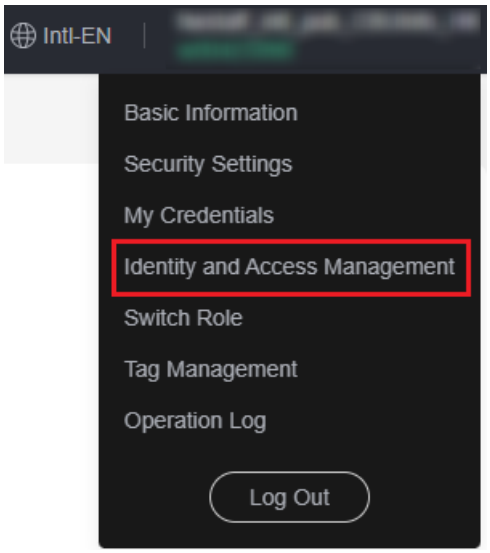
- You and all IAM users created using your account can access the **Security Settings** page from the management console.
  a. Log in to Huawei Cloud and click **Console** in the upper right corner.
  b. On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Security Settings** from the drop-down list.

  Figure 8-1 Going to the security settings page



- As an administrator, you can also access the **Security Settings** page from the IAM console.
  a. Log in to Huawei Cloud and click **Console** in the upper right corner.
  b. On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.

Figure 8-2 Accessing the IAM service



c. On the IAM console, choose **Security Settings** from the left navigation pane.

8.2 Basic Information

As an account administrator, both you and your IAM users can manage basic information on this page. You can also change your login password, mobile number, and email address by referring to **HUAWEI ID Information Management**.

NOTE

- A mobile number or an email address can be bound only to one account or IAM user.
- Only one mobile number, email address, and virtual MFA device can be bound to an account or IAM user.

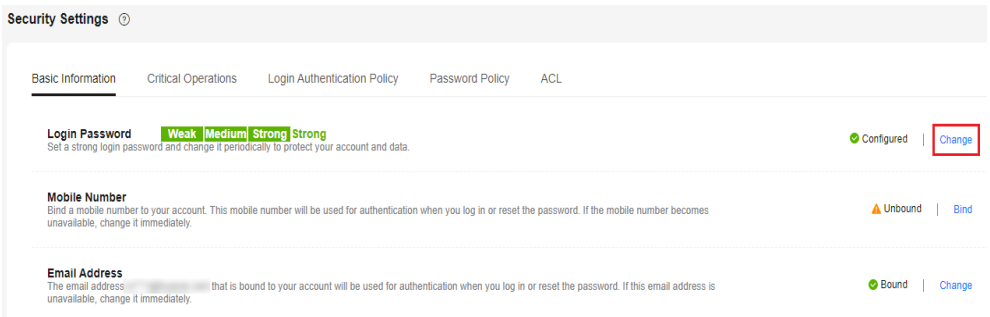
Changing the Login Password, Mobile Number, or Email Address

The methods for changing the login password, mobile number, and email address are similar. To change the login password, do as follows:

Step 1 Go to the **Security Settings** page.

Step 2 Click the **Basic Information** tab, and click **Change** in the **Login Password** row.

Figure 8-3 Changing the login password



Step 3 (Optional) Select email address or mobile number verification, and enter the verification code.

NOTE

If neither email address nor mobile number is bound, no verification is required.

Step 4 Enter the old password and new password, and enter the new password again.

NOTE

- The password cannot be the username or the username spelled backwards. For example, if the username is **A12345**, the password cannot be **A12345**, **a12345**, **54321A**, or **54321a**.
- To prevent password cracking, the administrator can configure the password policy to define password requirements, such as minimum password length. For details, see **Password Policy**.

Step 5 Click **OK**.

----End

8.3 Critical Operation Protection

Only an **administrator** can configure critical operation protection, and IAM users can only view the configurations. If an IAM user needs to modify the configurations, the user can request the administrator to perform the modification or grant the required permissions.

NOTE

Federated users do not need to verify their identity when performing critical operations.

Virtual MFA Device

An MFA device generates 6-digit verification codes in compliance with the Time-based One-time Password Algorithm (TOTP). MFA devices can be hardware- or software-based. Currently, only software-based virtual MFA devices are supported. They are application programs running on smart devices such as mobile phones.

This section describes how to bind a virtual MFA device, for example, the Huawei Cloud App. If you have installed another MFA application, add a user by following the on-screen prompts. For details about how to bind or remove a virtual MFA device, see **Configuring a Virtual MFA Device**.

The method for binding a virtual MFA device varies depending on whether your **Huawei Cloud account** has been upgraded to a **HUAWEI ID**.

NOTE

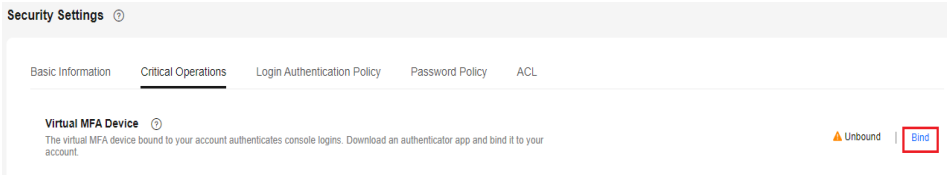
Before binding a virtual MFA device, ensure that you have installed an MFA application (such as an Authenticator app) on your mobile device.

- **Huawei Cloud account**

Step 1 Go to the **Security Settings** page.

Step 2 Click the **Critical Operations** tab, and click **Bind** in the **Virtual MFA Device** row.

Figure 8-4 Virtual MFA device



Step 3 Set up the MFA application by scanning the QR code or manually entering the secret key.

You can bind a virtual MFA device to your account by scanning the QR code or entering the secret key.

- Scanning the QR code

  Open the MFA application on your mobile phone, and use the application to scan the QR code displayed on the **Bind Virtual MFA Device** page. Your account or IAM user is then added to the application.

- Manually entering the secret key

  Open the MFA application on your mobile phone, and enter the secret key.

  NOTE

  The user can be manually added only using time-based one-time passwords (TOTP). You are advised to enable automatic time setting on your mobile device.

Step 4 View the verification codes on the MFA application. The code is automatically updated every 30 seconds.

Step 5 On the **Bind Virtual MFA Device** page, enter two consecutive verification codes and click **OK**.

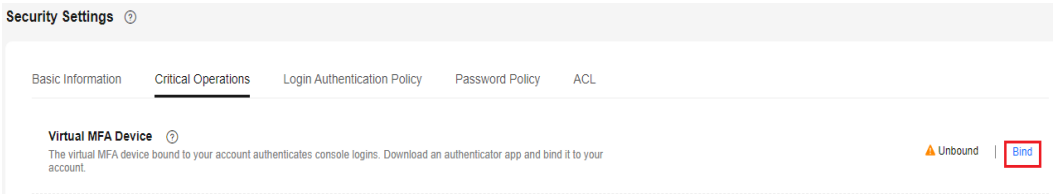
----End

- **HUAWEI ID**

Step 1 Go to the **Security Settings** page.

Step 2 Click the **Critical Operations** tab, and click **Bind** in the **Virtual MFA Device** row.

Figure 8-5 Binding a virtual MFA device



Step 3 On the **Account & security** page of the HUAWEI ID account center, associate an authenticator with your HUAWEI ID as instructed.

----End

Login Protection

After login protection is enabled, you and IAM users created using your account will need to enter a verification code in addition to the username and password during login. Enable this function for account security.

For an account, only the account administrator can enable login protection for it. For IAM users, both the account administrator and other administrators can enable this feature for the users.

- **(Administrator) Enabling login protection for an IAM user**

  To enable login protection for an IAM user, go to the **Users** page and choose **Security Settings** in the row that contains the IAM user. In the **Login Protection** area in the displayed **Security Settings** tab, click next to **Verification Method**, and select a verification method from SMS, email, or virtual MFA device or security key. You can enable or disable API login protection as needed when you select **Virtual MFA device**. The option is disabled by default. API login protection asks you for both a password and a virtual MFA device to obtain an IAM user's security token. Without API login protection, you can obtain the token with only a password. To obtain an IAM user token, see **Obtaining a User Token Through Password and Virtual MFA Authentication**.

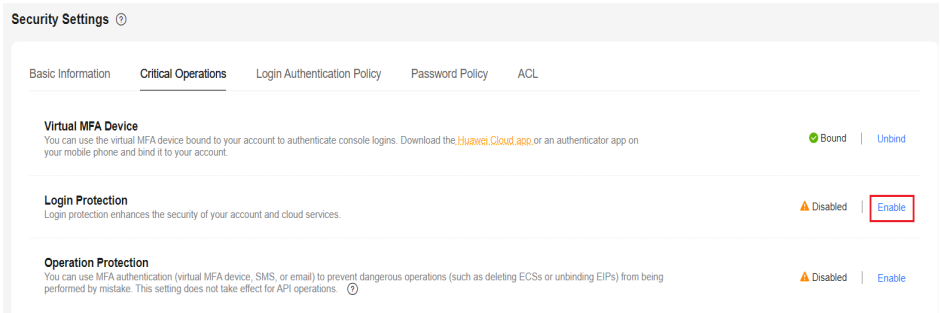
  NOTE

  After you enable login protection, IAM users need to perform identity verification when they access Huawei Cloud using the management console. The setting does not apply if IAM users use programmatic access.

- **Enabling login protection for your Huawei Cloud account**

  If your Huawei Cloud account has not been upgraded to a HUAWEI ID, you can enable login protection on the **Security Settings** page. Go to the **Security Settings** page, and click the **Critical Operations** tab. Click **Enable** next to **Login Protection**, select a verification method, enter the verification code, and click **OK**. You can enable or disable API login protection as needed when you select **Virtual MFA device**. The option is disabled by default. API login protection asks you for both a password and a virtual MFA device to obtain an IAM user's security token. Without API login protection, you can obtain the token with only a password.

  Figure 8-6 Enabling login protection

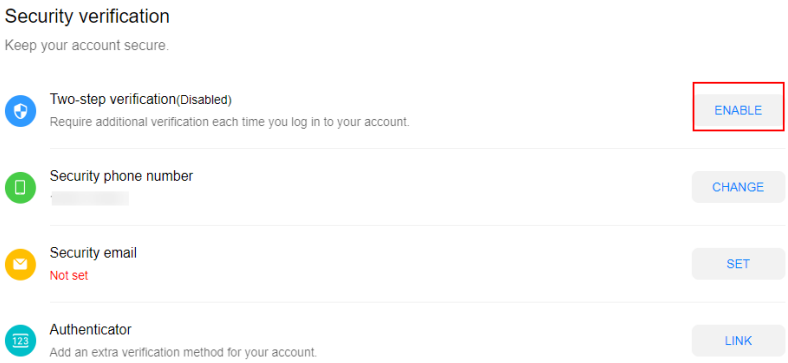
  

- **Enabling login protection for your HUAWEI ID**

  If your Huawei Cloud account has been upgraded to a HUAWEI ID, enable login protection in the HUAWEI ID account center. Go to the **HUAWEI ID**

account center, choose **Account & security**, locate **Two-step verification** in the **Security verification** area, click **ENABLE**, complete verification, and click **OK**.

Figure 8-7 Enabling login protection



The system authenticates your identity when you log in with a HUAWEI ID. If you use a new terminal to log in, you will be authenticated with your security phone number at first login. If two-step verification is not enabled, click **Trust** to add your terminal to the trust list. Then you will no longer need to perform authentication when logging in using this terminal next time.

Operation Protection

- **Enabling operation protection**

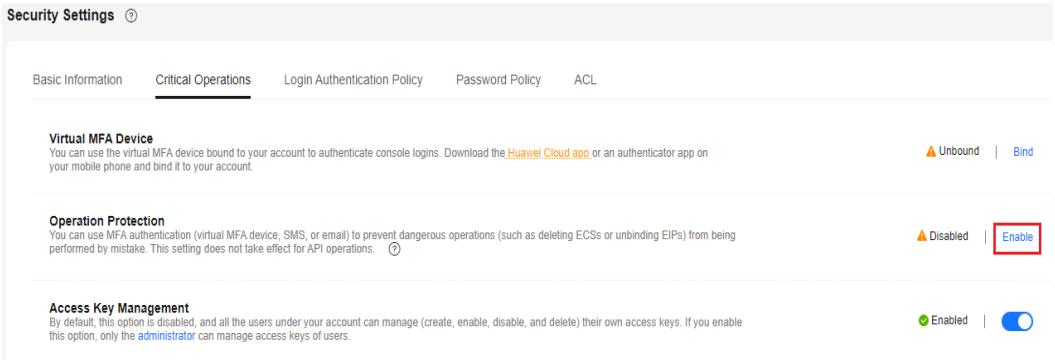
  After operation protection is enabled, you and IAM users created using your account need to enter a verification code when performing a **critical operation**, such as deleting an ECS. This function is enabled by default. To ensure resource security, keep it enabled.

  The verification is valid for 15 minutes and you do not need to be verified again when performing critical operations within the validity period.

Step 1 Go to the **Security Settings** page.

Step 2 On the **Critical Operations** tab, locate the **Operation Protection** row and click **Enable**.

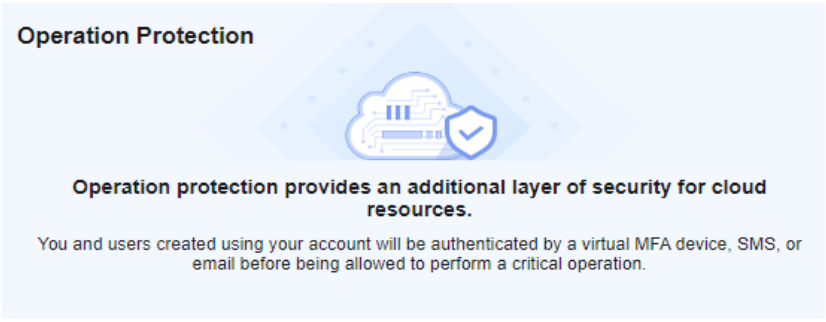
Figure 8-8 Enabling operation protection

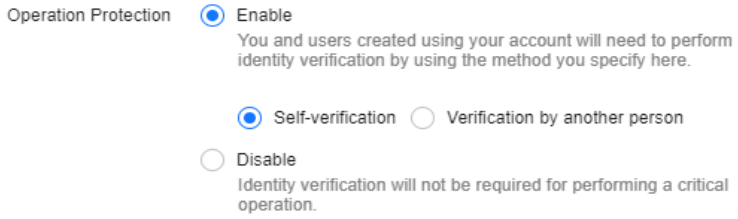


Step 3 Select **Enable** and then select **Self-verification** or **Verification by another person**.

If you select **Verification by another person**, an identity verification is required to ensure that this verification method is available.

Figure 8-9 Configuring operation protection





- **Self-verification**: You or IAM users themselves perform verification when performing a critical operation.
- **Verification by another person**: The specified person completes verification when you or IAM users perform a critical operation. Only SMS and email verification are supported.

Step 4 Click **OK**.

----End

- **Disabling operation protection**

If operation protection is disabled, you and IAM users created using your account do not need to enter a verification code when performing a **critical operation**.

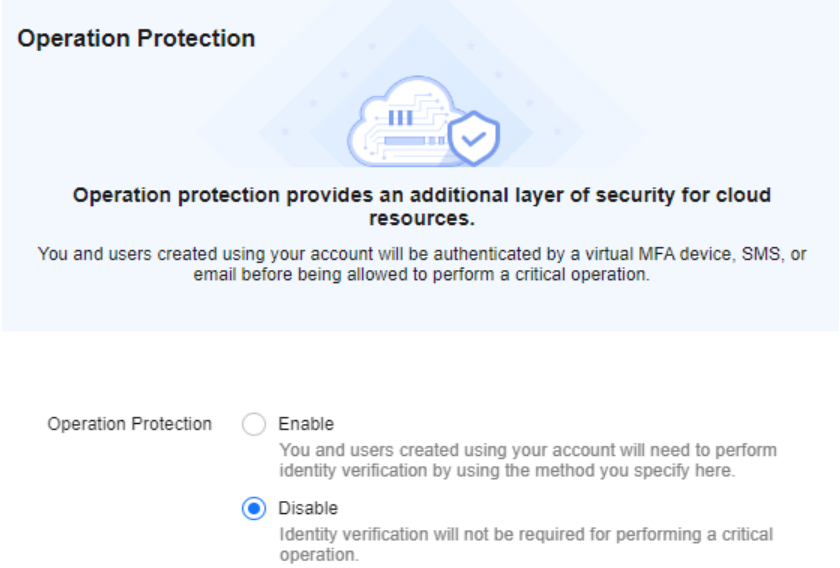
Step 1 Go to the **Security Settings** page.

Step 2 On the **Critical Operations** tab, locate the **Operation Protection** row and click **Change**.

Figure 8-10 Disabling operation protection

Step 3 Select **Disable** and click **OK**.

Figure 8-11 Disabling operation protection



Step 4 Enter a verification code.

- **Self-verification**: The administrator who wants to disable operation protection completes the verification. SMS, email, and virtual MFA verification are supported.
- **Verification by another person**: The specified person completes the verification. Only SMS and email verification are supported.

Step 5 Click **OK**.

----End

NOTE

- Each cloud service defines its own critical operations.
- When IAM users created using your account perform a critical operation, they will be prompted to choose a verification method from email, SMS, and virtual MFA device.
  - If a user is only associated with a mobile number, only SMS verification is available.
  - If a user is only associated with an email address, only email verification is available.
  - If a user is not associated with an email address, mobile number, or virtual MFA device, the user will need to associate at least one of them before they can perform any critical operations.
- You may not be able to receive email or SMS verification codes due to communication errors. In this case, you are advised to use a virtual MFA device for verification.
- You can change the mobile number or email address in **My Account** and change the **virtual MFA device** on the Security Settings page of the IAM console.
- If operation protection is enabled, IAM users need to enter verification codes when performing a critical operation. The verification codes are sent to the mobile number or email address bound to the IAM users.

Access Key Management

- **Enabling access key management**

After access key management is enabled, only the administrator can create, enable, disable, or delete access keys of IAM users. This function is disabled by default. To ensure resource security, enable this function.

To enable access key management, click the **Critical Operations** tab on the **Security Settings** page, and click  in the **Access Key Management** row.

- **Disabling access key management**

  After access key management is disabled, all IAM users can create, enable, disable, or delete their own access keys.

  To disable access key management, click the **Critical Operations** tab on the **Security Settings** page, and click  in the **Access Key Management** row.

Information Self-Management

- **Enabling information self-management**

  By default, information self-management is enabled, indicating that all IAM users can manage their own **basic information** (login password, mobile number, and email address). Determine whether to allow IAM users to manage their own information and what information they can modify.

  To enable information self-management, click the **Critical Operations** tab on the **Security Settings** page, and click **Enable** in the **Information Self-Management** row. Select **Enable**, select the information types that IAM users can modify, and click **OK**.

- **Disabling information self-management**

  After you disable information self-management, only administrators can manage their own **basic information**. If IAM users need to modify their login password, mobile number, or email address, they can contact the administrator. For details, see **Managing IAM User Information**.

  To disable information self-management, click the **Critical Operations** tab on the **Security Settings** page, and click **Change** in the **Information Self-Management** row. In the displayed pane, select **Disable** and click **OK**.

Critical Operations

The following tables list the critical operations defined by each cloud service.

Table 8-2 Critical operations defined by cloud services

Service Category	Service	Critical Operation
Compute	Elastic Cloud Server (ECS)	• Stopping, restarting, or deleting an ECS • Resetting the password for logging in to an ECS • Detaching a disk • Unbinding an EIP • Changing specifications without stopping an ECS • Changing the OS without stopping an ECS • Reinstalling the OS without stopping an ECS
Compute	Bare Metal Server (BMS)	• Stopping or restarting a BMS • Resetting the BMS password • Detaching a disk • Unbinding an EIP
Compute	Auto Scaling	Deleting an auto scaling group
Storage	Object Storage Service (OBS)	• Deleting a bucket • Creating, editing, or deleting a bucket policy • Configuring an object policy • Creating, editing, or deleting a bucket ACL • Configuring access logging • Configuring URL validation • Creating or editing a bucket inventory
Storage	Elastic Volume Service (EVS)	• Deleting an EVS disk • Deleting a snapshot • Unsubscribing from a yearly/monthly EVS disk
Storage	Cloud Backup and Recovery (CBR)	• Deleting a vault • Deleting a backup • Restoring a backup • Deleting a policy • Dissociating a resource • Accepting a backup
Storage	Scalable File Service (SFS)	Deleting an SFS Turbo file system

Service Category	Service	Critical Operation
Storage	Dedicated Distributed Storage Service (DSS)	Deleting a disk
CDN and Intelligent Edge	Content Delivery Network (CDN)	Configuring the service termination policy
Containers	Cloud Container Engine (CCE)	• Deleting a cluster • Unsubscribing from a cluster
Containers	Ubiquitous Cloud Native Service (UCS)	• Deleting a federation
Containers	Application Orchestration Service (AOS)	• Deleting a stack
Networking	Domain Name Service (DNS)	• Modifying, disabling, or deleting a record set • Modifying or deleting a PTR record • Deleting a custom line
Networking	Virtual Private Cloud (VPC)	• Releasing or unbinding an EIP • Deleting a VPC peering connection • Security group operations – Deleting an inbound or outbound rule – Modifying an inbound or outbound rule – Batch deleting inbound or outbound rules

Service Category	Service	Critical Operation
Networking	Elastic Load Balance (ELB)	• Shared load balancers – Deleting a load balancer – Deleting a listener – Deleting a certificate – Removing a backend server – Unbinding an EIP – Unbinding a public or private IPv4 address • Dedicated load balancers – Deleting a load balancer – Deleting a listener – Deleting a certificate – Removing a backend server – Unbinding an EIP – Unbinding a public or private IPv4 address – Unbinding an IPv6 address – Removing from IPv6 shared bandwidth
Networking	Elastic IP (EIP)	• Deleting a shared bandwidth • Releasing or unbinding an EIP • Batch releasing or unbinding EIPs
Networking	NAT Gateway (NAT)	• Private NAT gateways – Deleting an SNAT rule – Deleting a DNAT rule – Releasing a transit IP address • Public NAT gateways – Deleting an SNAT rule – Deleting a DNAT rule

Service Category	Service	Critical Operation
Networking	Virtual Private Network (VPN)	• Deleting or modifying a VPN connection • Unsubscribing from a yearly/monthly VPN gateway • Deleting or modifying a VPN gateway • Deleting or modifying a customer gateway • Changing the specification of a VPN gateway • Unbinding an EIP • Modifying a server • Deleting or modifying a server certificate • Deleting a client CA certificate • Creating, deleting, or modifying a user or user group • Batch deleting users • Creating, deleting, or modifying an access policy • Resetting a user password
Networking	Direct Connect	Deleting a virtual interface
Security & Compliance	Data Encryption Workshop (DEW)	• Deleting a key • Deleting a key alias • Revoking a key grant • Deleting a secret • Deleting a secret event • Deleting a key pair • Deleting a dedicated HSM cluster • Deleting a cryptographic cluster • Deleting a cryptographic application • Deleting a cryptographic key • Deleting a management policy • Deleting physical and environmental information

Service Category	Service	Critical Operation
Management & Governance	Identity and Access Management (IAM)	• Disabling operation protection • Disabling login protection • Changing the mobile number • Changing the email address • Changing the login password • Changing the login authentication method • Deleting an IAM user • Disabling an IAM user • Deleting an agency • Deleting a user group • Deleting a policy • Deleting permissions • Creating an access key • Deleting an access key • Disabling an access key • Deleting a project • Modifying the status of access key management
Management & Governance	Log Tank Service (LTS)	• Deleting a log stream or log group • Uninstalling the ICAgent
Management & Governance	Resource Formation Service (RFS)	Deleting a stack
Middleware	Distributed Cache Service (DCS)	• Resetting the password • Deleting a DCS instance • Clearing DCS instance data
Middleware	Distributed Message Service (DMS) for Kafka	Deleting an instance
Middleware	Distributed Message Service (DMS) for RabbitMQ	Deleting an instance
Middleware	Distributed Message Service (DMS) for RocketMQ	Deleting an instance

Service Category	Service	Critical Operation
Database	RDS for MySQL	• Resetting the administrator password • Deleting a DB instance • Deleting a database backup • Restoring a DB instance from a backup file • Restoring a DB instance to a point in time • Switching between primary and standby DB instances • Changing the database port • Deleting a database account • Deleting a database • Changing a floating IP address • Unbinding an EIP • Downloading a full backup • Downloading a Binlog backup • Changing a private domain name • Changing a public domain name • Modifying a host IP address • Stopping an instance • Starting an instance • Restarting an instance • Resetting a password for a database account
Database	RDS for PostgreSQL	• Resetting the administrator password • Deleting a DB instance • Deleting a database backup • Switching between primary and standby DB instances • Changing the database port • Changing a floating IP address • Unbinding an EIP • Downloading a full backup • Changing a private domain name • Downloading an incremental backup file • Restoring a DB instance from a backup file • Restoring a DB instance to a point in time

Service Category	Service	Critical Operation
Database	RDS for SQL Server	• Resetting the administrator password • Deleting a DB instance • Deleting a database backup • Switching between primary and standby nodes • Changing the database port • Deleting a database • Changing a floating IP address • Changing a private domain name • Changing a public domain name • Unbinding an EIP • Stopping an instance • Starting an instance • Restarting an instance • Downloading a full backup • Changing a private domain name • Downloading an incremental backup file • Restoring a DB instance from a backup file • Restoring a DB instance to a point in time
Database	TaurusDB	• Deleting a DB instance • Restarting a DB instance • Restarting a node • Deleting a read replica • Unbinding an EIP • Deleting a database • Resetting a password for a database account • Deleting a database account • Resetting the administrator password • Changing a private IP address • Restoring data to a specific point in time

Service Category	Service	Critical Operation
Database	Document Database Service (DDS)	• Resetting the password • Restarting or deleting a DB instance • Restarting a node • Switching the primary and secondary nodes of a replica set • Deleting a security group rule • Enabling IP addresses of shard and config nodes • Restoring the current DB instance from a backup • Restoring an existing DB instance from a backup • Changing a yearly/monthly instance to pay-per-use • Restoring instance- and table-level backups • Applying for a private domain name • Upgrading a minor version • Changing an AZ • Deleting a backup • Downloading backups • Deleting a read replica
Database	GeminiDB	• Restoring backup data to an existing instance • Clearing data • Deleting an account • Deleting a node • Shutting down a node • Changing the billing mode from yearly/monthly to pay-per-use • Releasing an instance • Unsubscribing from an instance • Deleting an instance • Deleting a dual-active relationship • Changing the billing mode from pay-per-use to yearly/monthly • Upgrading a minor version • Resetting the password • Restarting an instance

Service Category	Service	Critical Operation
Analytics	GaussDB(DWS)	• Scaling out a cluster • Changing all specifications • Binding an EIP • Deleting a cluster • Starting a cluster • Stopping a cluster • Adding or deleting a CN node • Upgrading clusters • Modifying cluster parameters • Deleting idle nodes • Enabling or disabling auto scaling • Rebooting an instance
Analytics	MapReduce Service (MRS)	• Clusters – Deleting a cluster – Changing a pay-per-use cluster to yearly/monthly billing – Stopping all components – Synchronizing cluster configurations • Nodes – Stopping all roles – Isolating a host – Canceling isolation of a host • Components – Disabling a service – Restarting a service – Performing a rolling service restart – Stopping a role instance – Restarting a role instance – Performing a rolling instance restart – Recommissioning a role instance – Decommissioning a role instance – Saving service configurations • Patches – Installing a patch – Uninstalling a patch – Rolling back a patch

Service Category	Service	Critical Operation
Business Applications	Workspace	• Workspaces – Unsubscribing from Huawei Cloud Workspace – Disabling Direct Connect access – Disabling Internet access – Changing a VPC – Deleting a desktop pool – Recomposing a system disk in a desktop pool – Deleting a disk from a desktop pool – Performing operations on a desktop pool (starting, stopping, restarting, and hibernating) – Executing a desktop pool script – Deleting a desktop – Performing operations on a desktop (starting, stopping, and restarting) – Rebuilding a desktop – Unbinding a user – Changing a desktop network – Migrating a desktop – Deleting an exclusive host – Unbinding an EIP from a desktop – Deleting a desktop snapshot – Restoring a desktop snapshot – Deleting a data disk from a desktop – Performing operations on a user (locking/unlocking a user and resetting a user password) – Deleting a user group – Deleting a policy group – Deleting a user – Deleting a desktop application – Deleting a site – Modifying the site access mode – Canceling Workspace bandwidth • Application streaming – Deleting an application group – Enabling an application

Service Category	Service	Critical Operation
		– Revoking application group authorization – Deleting a server group – Deleting a server – Reinstalling a server – Stopping a server – Deleting Workspace storage space – Deleting a personal storage directory – Deleting a policy group – Changing a server image
Business Applications	Message & SMS	• Deleting a signature • Deleting a template • Obtaining an app_secret • Binding a mobile number or an email address to your Huawei Cloud account • Configuring an IP address whitelist • Renewing a package
User Support	Billing Center	• Paying for an order • Unsubscribing from an order • Releasing resources

8.4 Login Authentication Policy

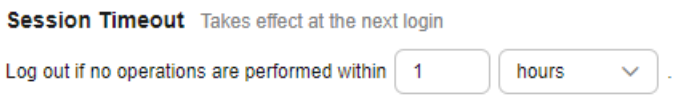
The **Login Authentication Policy** tab of the **Security Settings** page provides the **Session Timeout**, **Account Lockout**, **Account Disabling**, **Recent Login Information**, and **Custom Information** settings. These settings take effect for both your account and the IAM users created using the account.

Only the **administrator** can configure the login authentication policy, and IAM users can only view the configurations. If an IAM user needs to modify the configurations, the user can request the administrator to perform the modification or grant the required permissions.

Session Timeout

Set the session timeout that will apply if you or users created using your account do not perform any operations within a specific period.

Figure 8-12 Session Timeout

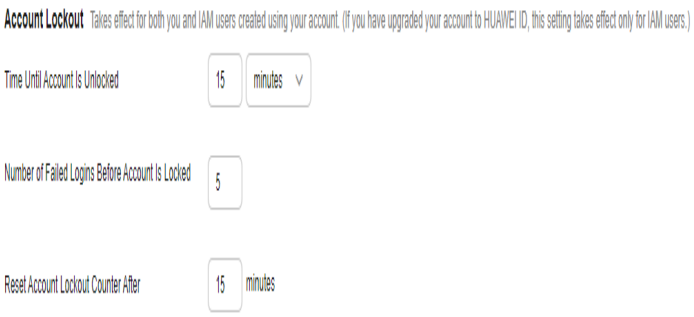


The timeout ranges from 15 minutes to 24 hours, and the default timeout is 1 hour.

Account Lockout

Set a duration to lock users out if a specific number of unsuccessful login attempts has been reached within a certain period. You cannot unlock your own account or an IAM user's account. Wait until the lock time expires.

Figure 8-13 Account Lockout



The administrator can set the account lockout duration, maximum number of unsuccessful login attempts before the account is locked, and time for resetting the account lockout counter.

- Lockout duration: The value range is from 15 to 30 minutes, and the default value is **15 minutes**.
- Maximum number of unsuccessful login attempts: The value range is from 3 to 10, and the default value is **5**.
- Time for resetting the account lockout counter: The value range is from 15 to 60 minutes, and the default value is **15 minutes**.

Account Disabling

Set a validity period to disable IAM users if they have not accessed Huawei Cloud using the console or APIs within a certain period.

This option is disabled by default. It can be enabled by the administrator. The validity period is from 1 day to 240 days.

If you enable this option, the setting will take effect only for IAM users created using your account. If an IAM user is disabled, the user can request the administrator to enable their account again.

Recent Login Information

Configure whether you want the system to display the previous login information after you log in. If incorrect login information is displayed on the **Login Verification** page, change your password immediately.

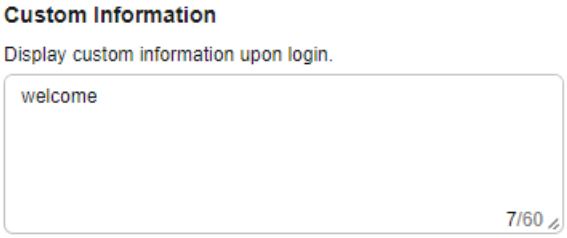
This option is disabled by default and can be enabled by the administrator.

Custom Information

Set custom information that will be displayed upon successful login. For example, enter the word **Welcome**.

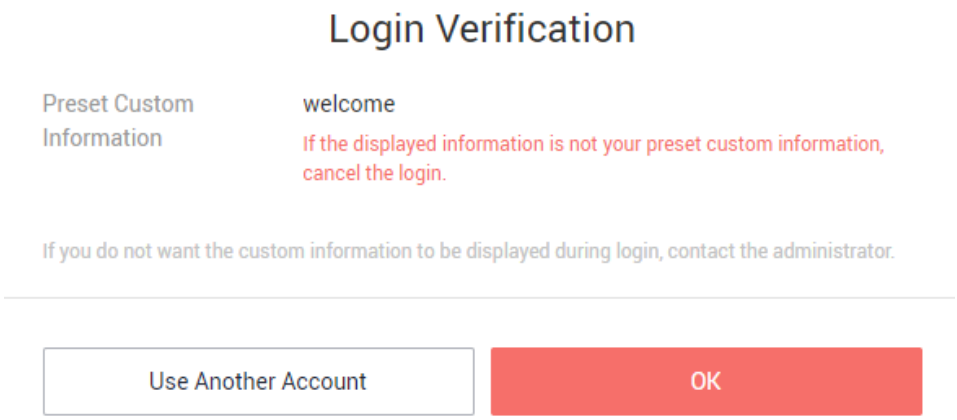
This option is disabled by default and can be enabled by the administrator.

Figure 8-14 Custom Information



You and all the IAM users created using your account will see the same information upon successful login.

Figure 8-15 Login verification



USB Key Certificate Expiration

To ensure service continuity, you can set a certificate expiration reminder to notify you of applying for a new USB key before the current one expires. The new USB key must be obtained within the certificate's validity time, or you will not be able to log in to the cloud platform after the current USB key expires. By default, you can receive a notification 10 days ahead of the expiration. You can set the notification time from 1 to 10 days.

This setting will be applied immediately for both your account and IAM users under your account.

8.5 Password Policy

The **Password Policy** tab of the **Security Settings** page provides the **Password Composition & Reuse**, **Password Expiration**, and **Minimum Password Age** settings.

Only the **administrator** can configure the password policy, and IAM users can only view the configurations. If an IAM user needs to modify the configurations, the user can request the administrator to perform the modification or grant the required permissions.

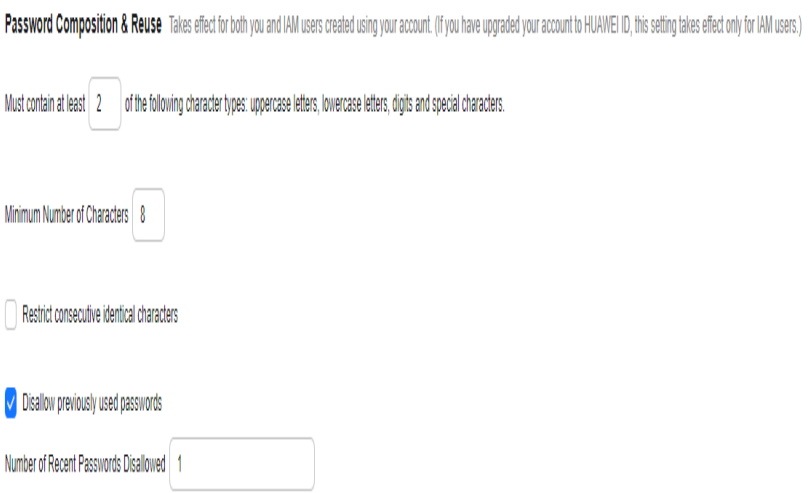
You can configure the password policy to ensure that IAM users create strong passwords and rotate them periodically. In the password policy, you can define password requirements, such as minimum password length, whether to allow consecutive identical characters in a password, and whether to allow previously used passwords.

NOTE

If your Huawei Cloud account has already been upgraded to a HUAWEI ID, the password policy does not take effect for the ID.

Password Composition & Reuse

Figure 8-16 Password Composition & Reuse



- Ensure that the password contains 2 to 4 of the following character types: uppercase letters, lowercase letters, digits, and special characters. By default, the password must contain at least 2 of these character types.
- Set the minimum number of characters that a password must contain. The default value is 8 and the value range is from 8 to 32.
- (Optional) Enable the **Restrict consecutive identical characters** option and set the maximum number of times that a character is allowed to be

consecutively present in a password. For example, value **1** indicates that consecutive identical characters are not allowed in a password.

- (Optional) Enable the **Disallow previously used passwords** option and set the number of previously used passwords that are not allowed. For example, value **3** indicates that the user cannot set the last three passwords that the user has previously used when setting a new password.

Changes to the password policy take effect the next time you or your IAM users change passwords. The new password policy will also apply to IAM users created later.

Password Expiration

Set a validity period for passwords so that users need to change their passwords periodically. The users will be prompted to change their passwords 15 days before password expiration. Expired passwords cannot be used to log in to Huawei Cloud.

This option is disabled by default. It can be enabled by the administrator. The validity period range is from 1 day to 180 days.

The changes will take effect immediately for your account and all IAM users under your account.

NOTE

After the password expires, users need to set a new password through the URL sent by email. The new password must be different from the old password.

Minimum Password Age

To prevent password loss due to frequent password changes, you can set a minimum period after which users are allowed to make a password change.

This option is disabled by default. The validity period ranges from 0 to 1,440 minutes.

The changes will take effect immediately for your account and all IAM users under your account.

8.6 ACL

The **ACL** tab of the **Security Settings** page provides the **IP Address Ranges**, **CIDR Blocks**, and **VPC Endpoints** settings for allowing user access only from specified IP address ranges, CIDR blocks, or VPC endpoints.

Only the **administrator** can configure the ACL to control access of all IAM users under the account from specific IP address ranges, CIDR blocks, or VPC endpoints.

Access type:

- **Console Access** (recommended): The ACL takes effect only for IAM users and federated users (SP-initiated)who are created using your account and have access to the console.
- **API Access**: The ACL controls users' API access through API Gateway and takes effect only for IAM users and federated users two hours after you complete the configuration.

NOTE

- You can configure a maximum of 200 access control items.
- If an IAM user or a federated user accesses Huawei Cloud through a proxy server, set the allowed IP addresses, address ranges or CIDR blocks based on the proxy IP address. If an IAM user or a federated user accesses Huawei Cloud through a public network, set based on the public IP address.
- Both IPv4 and IPv6 addresses can be used for console access, and only IPv4 addresses can be used for API access.

IP Address Ranges

Figure 8-17 IP address ranges

You can specify the IP address range to control access to Huawei Cloud. The IPv4 address range is from 0.0.0.0 to 255.255.255.255 and the default setting is 0.0.0.0-255.255.255.255. The IPv6 address range is from 0:0:0:0:0:0:0:0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and the default setting is 0:0:0:0:0:0:0:0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. If you do not specify a value range or use the default value range, IAM users can access Huawei Cloud from any IP addresses. To disable IPv6 access, set this the IP address to all zeros, for example, 0:0:0:0:0:0:0:0-0:0:0:0:0:0:0:0.

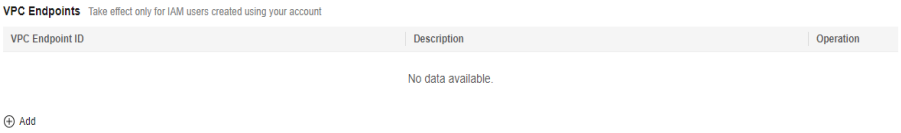
CIDR Blocks

Specify CIDR blocks to control access to Huawei Cloud. For example, set **CIDR Block** to **10.10.10.10/32**.

VPC Endpoints

Specify access to Huawei Cloud APIs only from the VPC Endpoint with the specified ID, for example, **0ccad098-b8f4-495a-9b10-613e2a5exxxx**. You can set the VPC endpoint only on the **API Access** tab. If access control is not configured, you can access APIs from all VPC endpoints by default.

Figure 8-18 VPC endpoints



NOTE

- User access is allowed if any of **IP Address Ranges**, **CIDR Blocks**, and **VPC Endpoints** is met.
- To restore **IP Address Ranges** to the default settings (0.0.0.0-255.255.255.255) and clear the settings in **CIDR Blocks** and **VPC Endpoints**, click **Restore Defaults**.

9 Identity Providers

9.1 Overview

Huawei Cloud provides identity federation based on Security Assertion Markup Language (SAML) or OpenID Connect. This function allows users in your enterprise management system to access Huawei Cloud through single sign-on (SSO).

Basic Concepts

Table 9-1 Basic concepts

Concept	Description
Identity provider (IdP)	An IdP collects and stores user identity information, such as usernames and passwords, and authenticates users during login. For identity federation between an enterprise and Huawei Cloud, the identity authentication system of the enterprise is an identity provider and is also called "enterprise IdP". Popular third-party IdPs include Microsoft Active Directory Federation Services (AD FS) and Shibboleth.
Service provider (SP)	A service provider establishes a trust relationship with an IdP and provides services based on the user information provided by the IdP. For identity federation between an enterprise and Huawei Cloud, Huawei Cloud is a service provider.
Identity federation	Identity federation is the process of **establishing a trust relationship** between an IdP and SP to implement SSO.

Concept	Description
Single sign-on (SSO)	SSO allows users to access a trusted SP after logging in to the enterprise IdP. For example, after a trust relationship is established between an enterprise management system and Huawei Cloud, users in the enterprise management system can use their existing accounts and passwords to access Huawei Cloud through the login link in the enterprise management system. Huawei Cloud supports two SSO types: virtual user SSO and IAM user SSO.
SAML 2.0	SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about an end user between an IdP and an SP. It is an open standard ratified by the Organization for the Advancement of Structured Information Standards (OASIS) and is being used by many IdPs. For more information about this standard, see **SAML 2.0 Technical Overview**. Huawei Cloud implements identity federation in compliance with SAML 2.0. To successfully federate your enterprise users with Huawei Cloud, ensure that your enterprise IdP is compatible with this protocol.
OpenID Connect	OpenID Connect is a simple identity layer on top of the Open Authorization 2.0 (OAuth 2.0) protocol. IAM implements identity federation in compliance with OpenID Connect 1.0. To successfully federate your enterprise users with Huawei Cloud, ensure that your enterprise IdP is compatible with this protocol. For more information about OpenID Connect, see **OpenID Connect Introduction**.
OAuth 2.0	OAuth 2.0 is an open authorization protocol. The authorization framework of this protocol allows third-party applications to obtain access permissions.

Advantages of Identity Federation

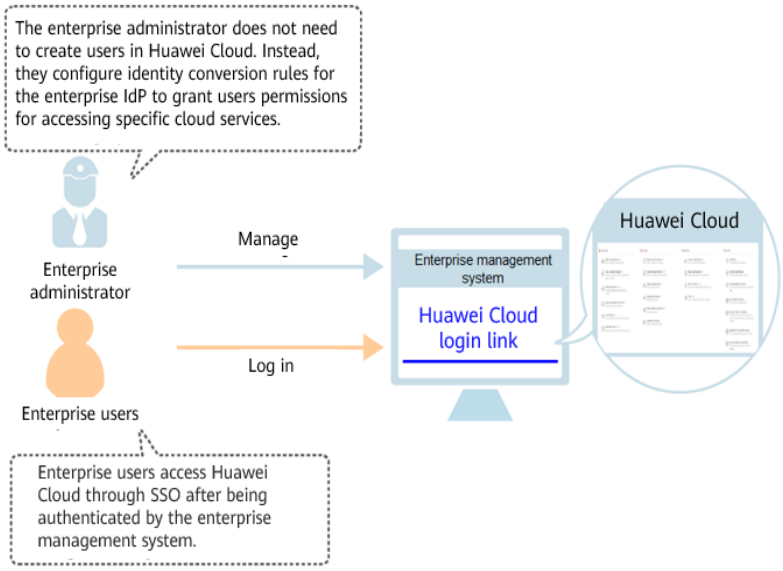
- Easy identity management

  With an identity provider, the administrator can manage workforce identities outside of Huawei Cloud and give these external workforce identities permissions to use resources on Huawei Cloud.

- Simplified operations

  Workforce users can use their existing accounts in the enterprise to access Huawei Cloud through SSO.

Figure 9-1 Advantages of identity federation



SSO Type

IAM supports two SSO types: virtual user SSO and IAM user SSO. For details about how to choose an SSO type, see **Application Scenarios of Virtual User SSO and IAM User SSO**.

- Virtual user SSO

  After a federated user logs in to Huawei Cloud, the system automatically creates a virtual user and grants access permissions to the virtual user based on the configured identity conversion rules.

- IAM user SSO

  After a federated user logs in to Huawei Cloud, the system automatically maps the **external identity ID** to an IAM user so that the federated user has the permissions of the mapped IAM user.

Currently, IAM supports two federated login methods: browser-based SSO (web SSO) and SSO via API calling.

- Web SSO: Browsers are used as the communication media. This authentication type enables common users to access Huawei Cloud using browsers. You can initiate web SSO from the IdP or SP side.
  - IdP-initiated SSO: **Configure a login link in the enterprise management system**. Your enterprise employees can use the link to log in to Huawei Cloud from the enterprise management system.
  - SP-initiated SSO: Huawei Cloud provides the **federated user login** entry. Your enterprise employees can enter a Huawei Cloud account and choose the enterprise's IdP on the login page to access Huawei Cloud.
- SSO via API calling: Enterprise employees call APIs using development tools (such as the OpenStack Client and Shibboleth ECP Client) to access Huawei Cloud.

Table 9-2 Federated logins

SSO Type	Supported Protocols	Web SSO	API Calling	IdP-initiated	SP-initiated	Multiple IdPs
Virtual user	SAML 2.0 and OpenID Connect	Supported	Supported	Supported	Supported	Supported
IAM user	SAML 2.0	Supported	Supported	Supported	Supported	Not supported

This chapter describes how to access Huawei Cloud through web SSO login. For details about how to access Huawei Cloud by calling APIs, see **Identity Federation Management**.

Precautions

- Ensure that your enterprise IdP server and Huawei Cloud use Greenwich Mean Time (GMT) time in the same time zone.
- The identity information (such as email address or mobile number) of federated users is stored in the enterprise IdP. Federated users are mapped to Huawei Cloud as virtual identities, so their access to Huawei Cloud has the following constraints:
  - Federated users do not need to perform a 2-step verification when performing critical operations even though **critical operation protection** (login protection or operation protection) is enabled.
  - Federated users cannot create access keys with unlimited validity, but they can obtain temporary access credentials (access keys and security tokens) using user or agency tokens. For details, see **Obtaining a Temporary Access Key and Security Token Through a Token**.

    If a federated user needs an access key with unlimited validity, they can contact the account administrator or an IAM user to create one. An access key contains the permissions granted to a user, so it is recommended that the federated user request an IAM user in the same group to create an access key.

9.2 Application Scenarios of Virtual User SSO and IAM User SSO

IAM supports two SSO types: virtual user SSO and IAM user SSO. This section describes the two SSO types and their differences, helping you to choose an appropriate type for your business.

Virtual User SSO

After a federated user logs in to Huawei Cloud, the system automatically creates a virtual user and assigns permissions to the user based on identity conversion rules. Virtual user SSO is recommended if:

- To reduce management costs, you do not want to create and manage IAM users on the cloud platform.
- You want to assign permissions for cloud resources based on the user groups or attributes in your local enterprise IdP. Permission changes in the local enterprise IdP can be synchronized to the cloud platform by adjusting the user groups or attributes locally.
- Your enterprise has branches and may require multiple enterprise IdPs. These IdPs need to access the same Huawei Cloud account. You need to configure multiple IdPs in Huawei Cloud for identity federation.

IAM User SSO

After a federated user logs in to Huawei Cloud, the system automatically maps the external identity ID to an IAM user so that the federated user has the permissions of the mapped IAM user. IAM user SSO is recommended if:

- The cloud products you use (such as **CodeArts**) do not support virtual user SSO.
- You do not need virtual user SSO and want to simplify the IdP configuration.

Differences Between Virtual User SSO and IAM User SSO

The differences between virtual user SSO and IAM user SSO are described as follows:

1. Identity conversion: Virtual user SSO uses **identity conversion rules** while IAM user SSO uses external identity IDs for identity conversion. If the **IAM_SAML_Attributes_xUserId** value of one or more IdP users is the same as the **external identity ID** of an IAM user, these IdP users will be mapped to the IAM user. When you use IAM user SSO, make sure that you have set **IAM_SAML_Attributes_xUserId** in the IdP and **External Identity ID** in the SP to the same value.

2. User identity in IAM: In virtual user SSO, the IdP user does not have a corresponding IAM user in the IAM user list. After the IdP user logs in, the system automatically creates a virtual user for it. In IAM user SSO, the IdP user has a IAM user mapped by external identity ID on the IAM console.

3. Permissions assignment in IAM: In virtual user SSO, the permissions of the IdP user are defined by the identity conversion rule. In IAM user SSO, the IdP user inherits the permissions of the user group which the mapped IAM user belongs to.

9.3 Virtual User SSO via SAML

9.3.1 Overview of Virtual User SSO via SAML

Huawei Cloud supports identity federation with Security Assertion Markup Language (SAML), which is an open standard that many identity providers (IdPs)

use. During identity federation, Huawei Cloud functions as a service provider (SP) and enterprises function as IdPs. This section describes how to configure identity federation and how identity federation works.

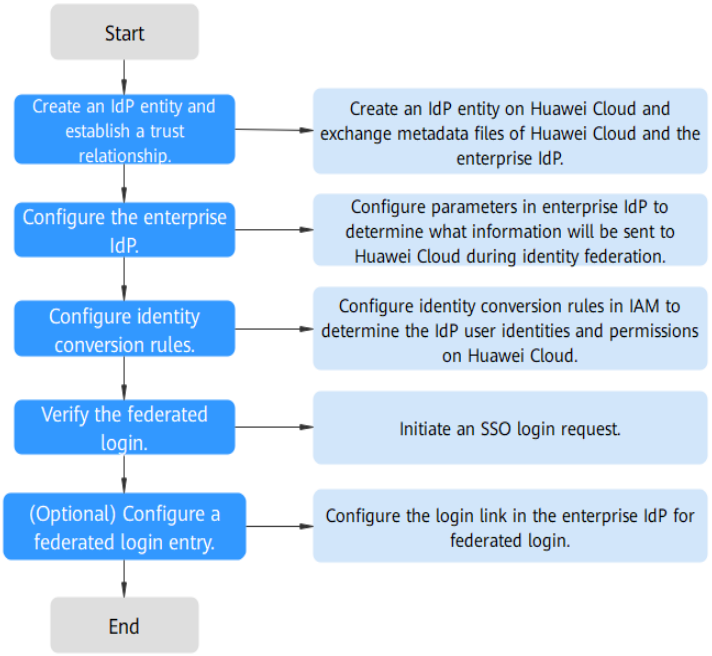
CAUTION

Ensure that your enterprise IdP supports SAML 2.0.

Configuring Identity Federation

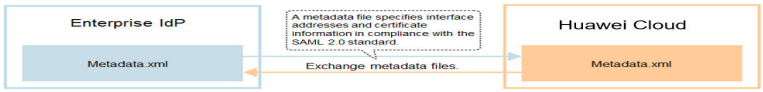
The following describes how to configure your enterprise IdP and Huawei Cloud to trust each other.

Figure 9-2 Configuration of virtual user SSO via SAML



1. **Create an IdP entity and establish a trust relationship**: Create an IdP entity for your enterprise on Huawei Cloud. Then, upload the Huawei Cloud metadata file to the enterprise IdP, and upload the metadata file of the enterprise IdP to Huawei Cloud.

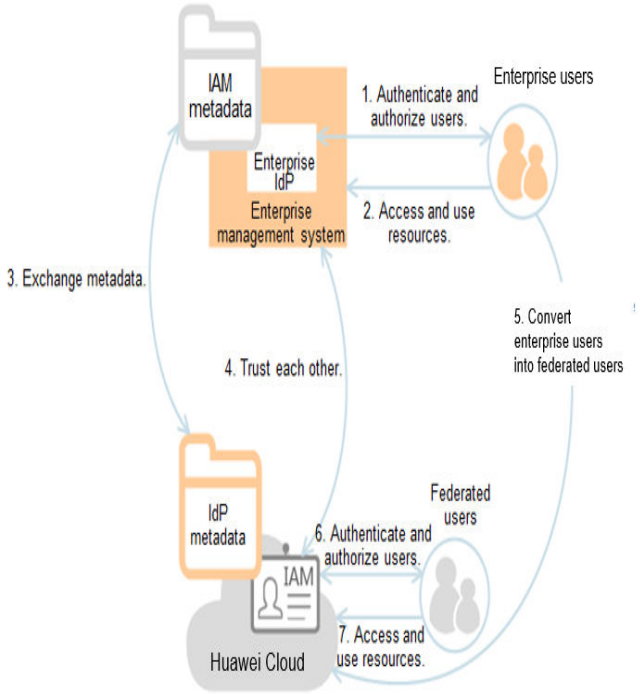
   Figure 9-3 Exchanging metadata files

2. **Configure the enterprise IdP**: Configure enterprise IdP parameters to determine what information can be sent to Huawei Cloud.

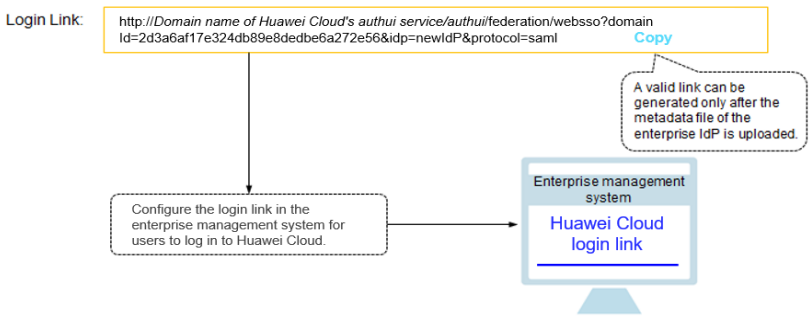
3. **Configure identity conversion rules on Huawei Cloud**: Configure identity conversion rules to determine the IdP user identities and permissions on Huawei Cloud.

Figure 9-4 Mapping external identities to virtual users



4. **Verify the federated login**: Check whether the enterprise user can log in to Huawei Cloud through SSO.
5. **(Optional) Configure a federated login entry**: Configure the login link (see **Figure 9-5**) in the enterprise IdP to allow enterprise users to be redirected to Huawei Cloud from your enterprise management system.

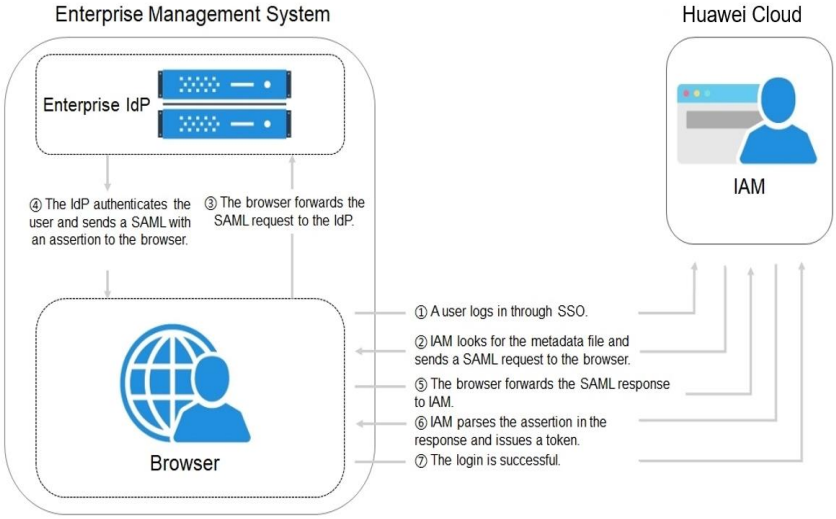
Figure 9-5 SSO login model



How Identity Federation Works

Figure 9-6 shows the identity federation process between an enterprise management system and Huawei Cloud.

Figure 9-6 How identity federation works



NOTE

To view interactive requests and assertions with a better experience, you are advised to use Google Chrome and install SAML Message Decoder.

As shown in Figure 9-6, the process of identity federation is as follows:

1. A user opens the login link generated after the IdP creation in the browser. The browser sends an SSO request to Huawei Cloud.
2. Huawei Cloud authenticates the user against the metadata file of the enterprise IdP and constructs a SAML request to the browser.
3. The browser forwards the SAML request to the enterprise IdP.
4. The user enters their username and password on the login page. After the enterprise IdP authenticates the user's identity, it constructs a SAML assertion containing the user details and sends the assertion to the browser as a SAML response.
5. The browser responds and forwards the SAML response to Huawei Cloud.
6. Huawei Cloud parses the assertion in the SAML response, identifies the IAM user group mapping to the user based on the identity conversion rules, and issues a token to the user.
7. The SSO login is successful.

NOTE

The assertion must carry a signature; otherwise, the login will fail.

9.3.2 Creating an IdP Entity

To establish a trust relationship between an enterprise IdP and Huawei Cloud, upload the metadata file of Huawei Cloud to the enterprise IdP, and then create

an IdP entity and upload the metadata file of the enterprise IdP on the IAM console.

Prerequisites

The enterprise administrator has read the help documentation of the enterprise IdP or has understood how to use the enterprise IdP. Configurations of different enterprise IdPs differ greatly, so they are not described in this document. For details about how to obtain the enterprise IdP's metadata file and how to upload the metadata file of Huawei Cloud to the enterprise IdP, see the IdP help documentation.

Establishing a Trust Relationship Between the Enterprise IdP and Huawei Cloud

The metadata file of Huawei Cloud needs to be configured in the enterprise IdP to establish a trust relationship between the two systems.

Step 1 Download the metadata file of Huawei Cloud.

Visit **https://auth-intl.huaweicloud.com/authui/saml/metadata.xml** (Google Chrome is recommended). Download the Huawei Cloud metadata file and set the file name, for example, **SP-metadata.xml**.

Step 2 Upload the metadata file to the enterprise IdP server. For details, see the help documentation of the enterprise IdP.

Step 3 Obtain the metadata file of the enterprise IdP. For details, see the help documentation of the enterprise IdP.

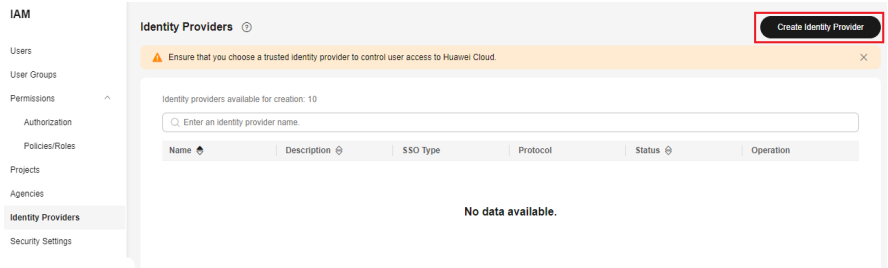
----End

Creating an IdP Entity on Huawei Cloud

To create an IdP entity on the IAM console, do as follows:

Step 1 Log in to the **IAM console**, choose **Identity Providers** from the navigation pane, and click **Create Identity Provider** in the upper right corner.

Figure 9-7 Creating an IdP entity



Step 2 Specify the name, protocol, SSO type, status, and description of the IdP entity.

Figure 9-8 Setting IdP parameters

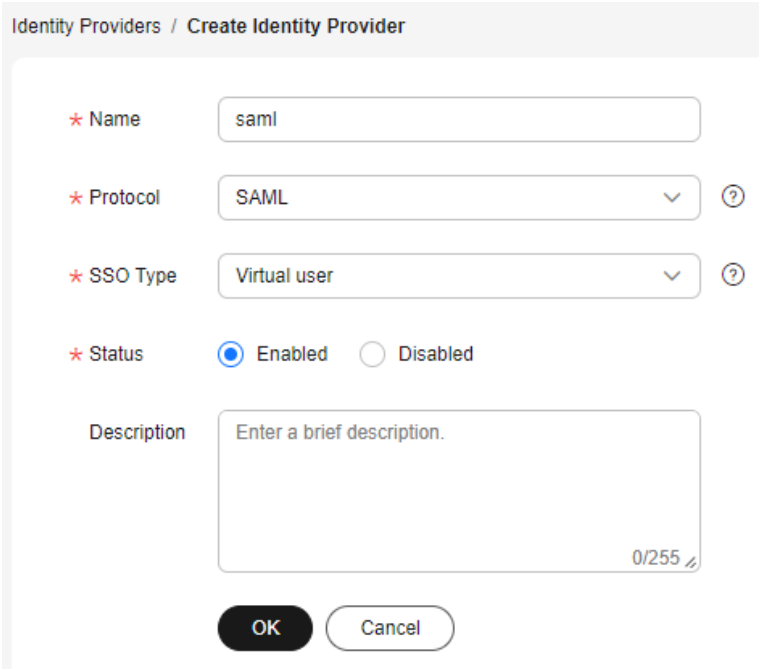


Table 9-3 Basic parameters of an IdP

Parameter	Description
Name	IdP name, which must be unique globally. You are advised to use the domain name.
Protocol	IdP protocol. Huawei Cloud supports SAML and OpenID Connect protocols. For details about OpenID Connect-based identity federation, see **Virtual User SSO via OpenID Connect**.
SSO Type	IdP type. An account can have only one type of IdP. The following describes the virtual user type. Virtual user SSO: After a federated user logs in to Huawei Cloud, the system automatically creates a virtual user for the federated user. An account can have multiple IdPs of the virtual user type.
Status	IdP status. The default value is **Enabled**.

Step 3 Click **OK**.

----End

Configuring the Metadata File of the Enterprise IdP on Huawei Cloud

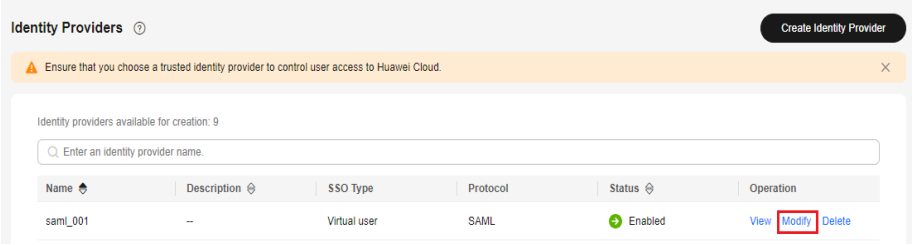
To configure the metadata file of the enterprise IdP in Huawei Cloud, you can upload the metadata file or manually edit metadata on the IAM console. For a metadata file larger than 500 KB, manually configure the metadata. If the metadata has been changed, upload the latest metadata file or edit the existing metadata to ensure that the federated users can log in to Huawei Cloud successfully.

NOTE

For details about how to obtain the metadata file of an enterprise IdP, see the help documentation of the enterprise IdP.

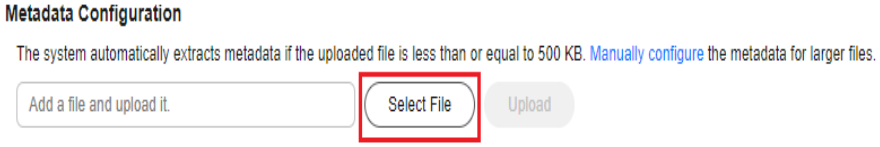
- **Upload a metadata file.**
  a. Click **Modify** in the row containing the IdP.

  Figure 9-9 Modifying an IdP

  b. Click **Select File** and select the metadata file of the enterprise IdP.

  Figure 9-10 Uploading a metadata file

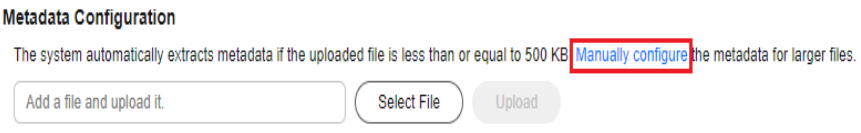
  

  c. Click **Upload**. The metadata extracted from the uploaded file is displayed. Click **OK**.

  - If the uploaded metadata file contains multiple IdPs, select the IdP you want to use from the **Entity ID** drop-down list.
  - If a message is displayed indicating that no entity ID is specified or the signing certificate has expired, check the metadata file and upload it again, or configure the metadata manually.

  d. Click **OK**.
- **Manually configure metadata.**
  a. Click **Manually configure**.

  Figure 9-11 Manually configuring metadata

  b. In the **Configure Metadata** dialog box, set the metadata parameters, such as **Entity ID**, **Signing Certificate**, and **SingleSignOnService**.

Parameter	Mandatory	Description
Entity ID	Yes	The unique identifier of an IdP. Enter the value of **entityID** displayed in the enterprise IdP's metadata file. If the metadata file contains multiple IdPs, choose the one you want to use.
Protocol	Yes	Protocol used for identity federation between an enterprise IdP and SP. The protocol is selected by default.
NameIdFormat	No	Enter the value of **NameIdFormat** displayed in the IdP metadata file. It specifies the username identifier format supported by the IdP, which is used for communication between the IdP and federated user. If you configure multiple values, Huawei Cloud uses the first value by default.
Signing Certificate	Yes	Enter the value of **<X509Certificate>** displayed in the IdP metadata file. A signing certificate is a public key certificate used for signature verification. For security purposes, enter a public key containing at least 2,048 bits. The signing certificate is used during identity federation to ensure that assertions are credible and complete. If you configure multiple values, Huawei Cloud uses the first value by default.

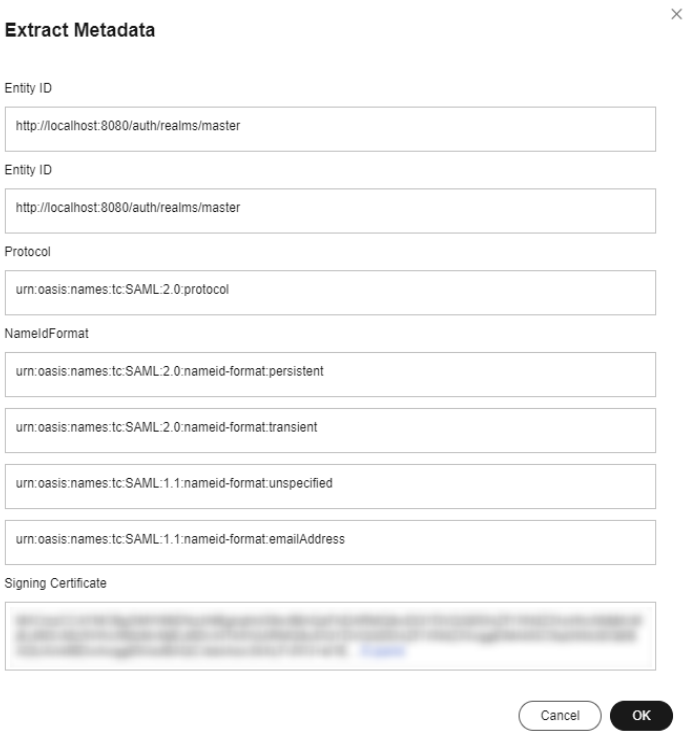
Parameter	Mandatory	Description
SingleSignOnService	Yes	Enter the value of **SingleSignOnService** displayed in the IdP metadata file. This parameter defines how SAML requests are sent during SSO. It must support HTTP Redirect or HTTP POST. If you configure multiple values, Huawei Cloud uses the first value by default.
SingleLogoutService	No	Enter the value of **SingleLogoutService** displayed in the IdP metadata file. This parameter indicates the address to which federated users will be redirected after logging out their sessions. It must support HTTP Redirect or HTTP POST. If you configure multiple values, Huawei Cloud uses the first value by default.

The following example shows the metadata file of an enterprise IdP and the manually configured metadata.

Figure 9-12 Metadata file of an enterprise IdP

```
<md:EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:names
:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Name="urn:keycloak">
    <md:EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:nam
es:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="http://localhost:8080/auth/realms/master">
        <md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <md:KeyDescriptor use="signing">
                <ds:KeyInfo>
                    <ds:KeyName>                                                    </ds:KeyName>
                    <ds:X509Data>
                        <ds:X509Certificate>
                                                                                    </ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </md:KeyDescriptor>
            <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://localhost:8080/auth/realms/master
/protocol/saml"/>
            <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://localhost:8080/auth/realms/ma
ster/protocol/saml"/>
            <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
            <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
            <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
            <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
            <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://localhost:8080/auth/realms/master
/protocol/saml"/>
            <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://localhost:8080/auth/realms/ma
ster/protocol/saml"/>
            <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="http://localhost:8080/auth/realms/master/prot
ocol/saml"/>
        </md:IDPSSODescriptor>
    </md:EntityDescriptor>
</md:EntitiesDescriptor>
```


Figure 9-13 Manually configuring metadata



c. Click **OK**.

Related Operations

- Viewing IdP information: In the IdP list, click **View** in the row containing the IdP, and view its basic information, metadata, and identity conversion rules.

  NOTE

  To modify the configuration of an IdP, click **Modify** at the bottom of the details page.

- Modifying an IdP: In the IdP list, click **Modify** in the row containing the IdP, and then change its status or modify the description, metadata, or identity conversion rules.
- Deleting an IdP: In the IdP list, click **Delete** in the row containing the IdP, and click **OK** in the displayed dialog box.

Follow-Up Procedure

- Configure the enterprise IdP: Configure enterprise IdP parameters to determine what information can be sent to Huawei Cloud.
- Configure identity conversion rules: In the **Identity Conversion Rules** area, configure identity conversion rules to establish a mapping between enterprise users and IAM user groups. In this way, enterprise users can obtain the corresponding permissions in Huawei Cloud. For details, see **Configuring Identity Conversion Rules**.
- Verify the federated login: Check whether the enterprise user can log in to Huawei Cloud through SSO. For details, see **Verifying the Login**.

9.3.3 Configuring an Enterprise IdP

You can configure parameters in the enterprise IdP to determine what information will be sent to Huawei Cloud. Huawei Cloud authenticates the federated identity and assigns permissions based on the received information and identity conversion rules.

Common Parameters in an Enterprise IdP

Table 9-4 Common parameters in an enterprise IdP

Parameter	Description	Scenario
IAM_SAML_Attributes_redirect_url	Target URL which the federated user will be redirected to	During SSO login, the federated user will be redirected to a page on Huawei Cloud, for example, the Cloud Eye homepage in the CN-Hong Kong region.
IAM_SAML_Attributes_domain_id	Account ID of Huawei Cloud to be federated with the enterprise IdP	This parameter is mandatory in the enterprise IdP-initiated federation.
IAM_SAML_Attributes_idp_id	Name of the IdP entity created on Huawei Cloud	This parameter is mandatory in the enterprise IdP-initiated federation.

9.3.4 Configuring Identity Conversion Rules

After an enterprise IdP user logs in to Huawei Cloud, Huawei Cloud authenticates the identity and assigns permissions to the user based on the identity conversion rules. You can customize identity conversion rules based on your service requirements. If you do not configure identity conversion rules, the username of the federated user on Huawei Cloud is **FederationUser** by default, and the federated user can only access Huawei Cloud by default.

You can configure the following parameters for federated users:

- Username: Usernames of federated users in Huawei Cloud.
- User permissions: Permissions assigned to federated users in Huawei Cloud. You need to map the federated users to IAM user groups. In this way, the federated users can obtain the permissions of the user groups to use Huawei Cloud resources. Ensure that user groups have been created. For details about how to create a user group, see **Creating a User Group and Assigning Permissions**.

NOTE

- Modifications to identity conversion rules will take effect the next time federated users log in.
- To modify the permissions of a user, modify the permissions of the user group which the user belongs to. Then restart the enterprise IdP for the modifications to take effect.

Prerequisites

- The enterprise administrator has created an account in Huawei Cloud, and has created user groups and assigned permissions to the group in IAM. For details, see **Creating a User Group and Assigning Permissions**.
- An IdP has been created in Huawei Cloud. For details, see **Creating an IdP Entity**.

Procedure

If you configure identity conversion rules by clicking **Create Rule**, IAM converts your specified parameters to the JSON format. Alternatively, you can click **Edit Rule** to configure rules in JSON format. For details, see **Syntax of Identity Conversion Rules**.

- **Creating Rules**
  a. Log in to the **IAM console** as the administrator. In the navigation pane, choose **Identity Providers**.
  b. In the IdP list, click **Modify** in the row containing the IdP.
  c. In the **Identity Conversion Rules** area, click **Create Rule**. Then, configure the rules in the **Create Rule** dialog box.

Figure 9-14 Creating rules

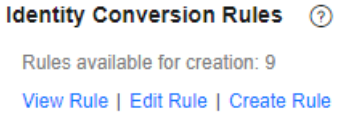


Figure 9-15 Creating rules

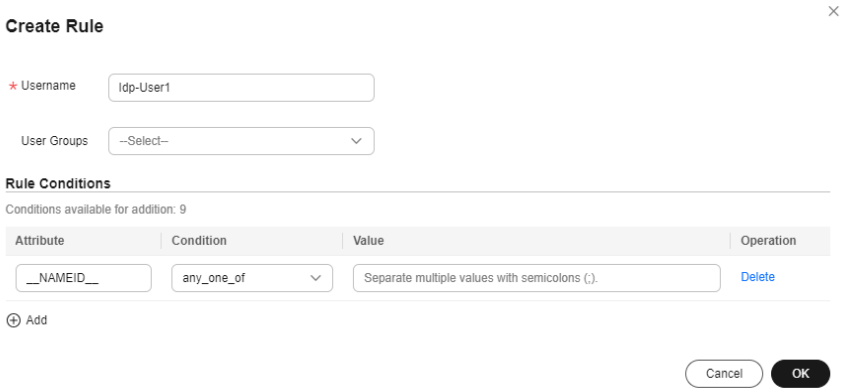


Table 9-5 Parameter description

Parameter	Description	Remarks
Username	Username of federated users in Huawei Cloud.	To distinguish federated users from Huawei Cloud users, it is recommended that you set the username to **FederationUser-***IdP_XXX*. *IdP* indicates an IdP name, for example, AD FS or Shibboleth. *XXX* indicates a custom name. **NOTICE** • The username of each federated user must be unique in the same IdP. Federated users with the same usernames in the same IdP will be mapped to the same IAM user in Huawei Cloud. • The username can only contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.). It cannot start with a digit and cannot contain the following special characters: ", \", \\, \n, \r
User Groups	User groups that the federated users belong to in Huawei Cloud.	The federated users will inherit permissions from their user groups. You can select a user group that has already been created.
Rule Conditions	Conditions that a federated user must meet to obtain permissions from the selected user groups.	Federated users who do not meet these conditions cannot access Huawei Cloud. You can create a maximum of 10 conditions for an identity conversion rule. The **Attribute** and **Value** parameters are used for the enterprise IdP to transfer user information to Huawei Cloud through SAML assertions. The **Condition** parameter can be set to **empty**, **any_one_of**, or **not_any_of**. For details about these parameters, see **Syntax of Identity Conversion Rules**. **NOTE** • An identity conversion rule can have multiple conditions. It takes effect only if all of the conditions are met. • An IdP can have multiple identity conversion rules. If a federated user does not meet any of the conditions, the user will be denied to access Huawei Cloud.

For example, set an identity conversion rule for administrators in the enterprise management system.

- Username: **FederationUser-IdP_admin**
- User group: **admin**
- Rule condition: **_NAMEID_** (attribute), **any_one_of** (condition), and **000000001** (value).

  Only the user with ID 000000001 is mapped to IAM user **FederationUser-IdP_admin** and inherits permissions from the **admin** user group.

d. In the **Create Rule** dialog box, click **OK**.

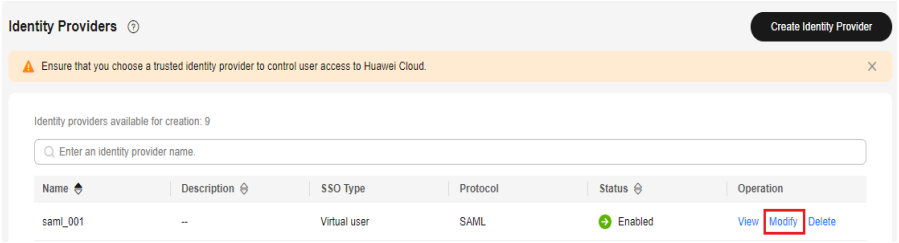
e. On the **Modify Identity Provider** page, click **OK**.

- **Editing Rules**

a. Log in to the **IAM console** as the administrator. In the navigation pane, choose **Identity Providers**.

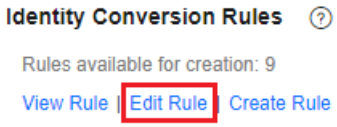
b. In the IdP list, click **Modify** in the row containing the IdP.

Figure 9-16 Modifying an IdP



c. In the **Identity Conversion Rules** area, click **Edit Rule**.

Figure 9-17 Editing identity conversion rules



d. Edit the identity conversion rules in JSON format. For details, see **Syntax of Identity Conversion Rules**.

e. Click **Validate** to verify the syntax of the rules.

f. If the rule is correct, click **OK** in the **Edit Rule** dialog box, and click **OK** on the **Modify Identity Provider** page.

If a message indicating that the JSON file is incomplete is displayed, modify the statements or click **Cancel** to cancel the modifications.

Related Operations

Viewing identity conversion rules: Click **View Rule** on the **Modify Identity Provider** page. The identity conversion rules are displayed in JSON format. For details about the JSON format, see **Syntax of Identity Conversion Rules**.

9.3.5 Verifying the Login

Verifying the Federated Login

Federated users can initiate a login from the IdP or SP.

- Initiating a login from an IdP, for example, Microsoft Active Directory Federation Services (AD FS) or Shibboleth.
- Initiating a login from the SP (Huawei Cloud). You can obtain the login link from the IdP details page on the IAM console.

The IdP-initiated login method depends on the IdP. For details, see the IdP help documentation. This section describes how to initiate a login from the SP.

Step 1 Log in as a federated user.

On the **Identity Providers** page of the IAM console, click **View** in the row containing the IdP. Click to copy the login link displayed in the **Basic Information** area, open the link using a browser, and then enter the username and password used in the enterprise management system.

Figure 9-18 Login link

Step 2 Check that the federated user has the permissions assigned to their user group.

----End

Redirecting to a Specified Region or Service

You can specify the target page which the federated user will be redirected to after login, for example, the Cloud Eye homepage in the CN-Hong Kong region.

- Configuring the login link on the SP

  Combine the login link obtained from the console with the specified URL using the format **Login link&service=Specified URL**. For example, if the obtained login link is **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml** and the specified URL is **https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**, the login link configured on the SP is https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml&service=**https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**
- Configuring the login link on the IdP

Configure **IAM_SAML_Attributes_redirect_url** (the URL to be redirected to) in the SAML assertion of the enterprise IdP.

9.3.6 Configuring a Federated Login Entry in the Enterprise IdP

Configure a federated login entry in the enterprise IdP so that enterprise users can use the login link to access Huawei Cloud.

NOTE

If no login link has been configured in your enterprise management system, federated users in your enterprise can log in to Huawei Cloud through the Huawei Cloud login page. For details, see **Logging In as a Federated User**.

Prerequisites

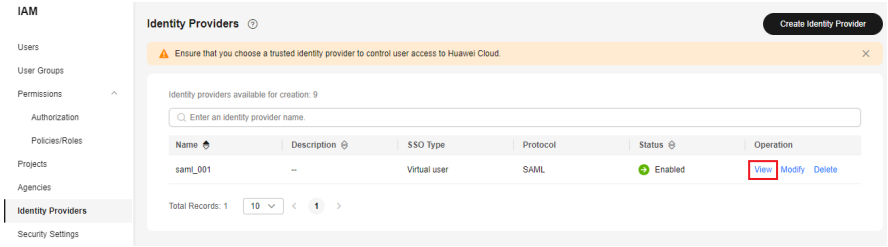
- An IdP entity has been created on Huawei Cloud. For details about how to create an IdP entity, see **Creating an IdP Entity**.
- The login entry for logging in to Huawei Cloud has been configured in the enterprise management system.

Procedure

Step 1 Log in to the **IAM console**. In the navigation pane, choose **Identity Providers**.

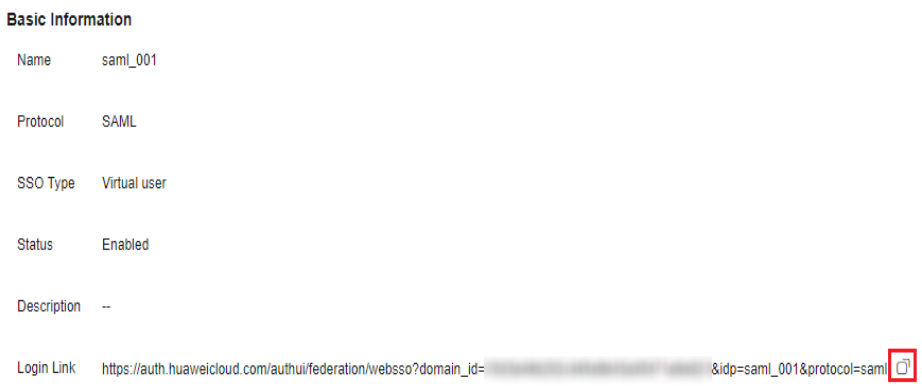
Step 2 Click **View** in the row containing the IdP.

Figure 9-19 Viewing IdP details



Step 3 Copy the login link by clicking in the **Login Link** row.

Figure 9-20 Copying the login link



Step 4 Add the following statement to the page file of the enterprise management system:

```
<a href="<Login link>"> Huawei Cloud login entry </a>
```

Step 5 Log in to the enterprise management system using your enterprise account, and click the configured login link to access Huawei Cloud.

----End

9.4 IAM User SSO via SAML

9.4.1 Overview of IAM User SSO via SAML

Huawei Cloud supports identity federation with Security Assertion Markup Language (SAML), which is an open standard that many identity providers (IdPs) use. During identity federation, Huawei Cloud functions as a service provider (SP) and enterprises function as IdPs. SAML-based federation enables single sign-on (SSO), so employees in your enterprise can log in to Huawei Cloud as IAM users.

This section describes how to configure identity federation and how identity federation works.

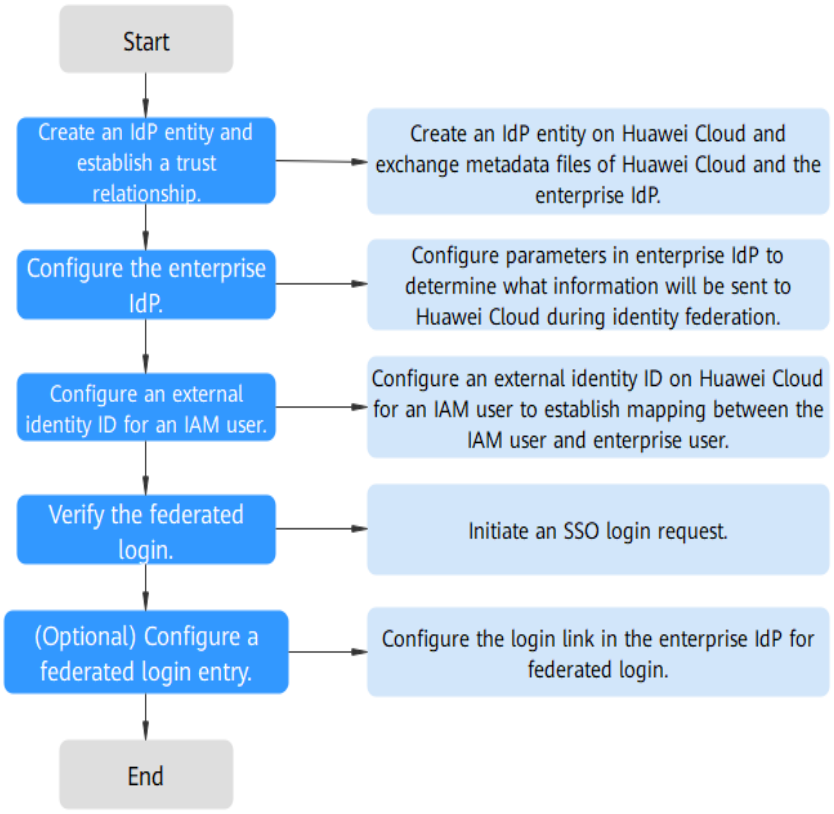
CAUTION

Ensure that your enterprise IdP supports SAML 2.0.

Configuring Identity Federation

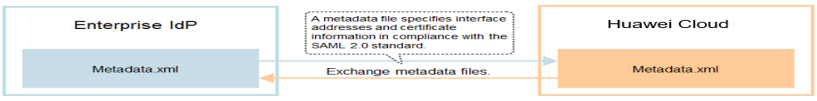
The following describes how to configure your enterprise IdP and Huawei Cloud to trust each other.

Figure 9-21 Configuration of IAM user SSO via SAML



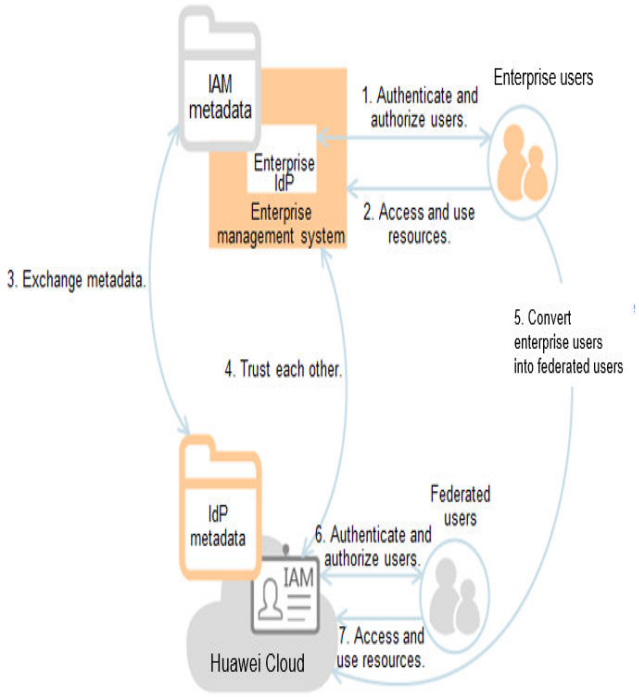
1. **Create an IdP entity and establish a trust relationship**: Create an IdP entity for your enterprise on Huawei Cloud. Then, upload the Huawei Cloud metadata file to the enterprise IdP, and upload the metadata file of the enterprise IdP to Huawei Cloud.

   Figure 9-22 Exchanging metadata files

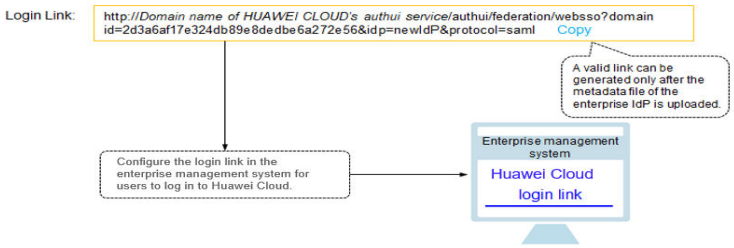
2. **Configure the enterprise IdP**: Configure enterprise IdP parameters to determine what information can be sent to Huawei Cloud.
3. **Configure an external identity ID**: Establish a mapping between an IAM user and an enterprise user. When your enterprise IdP establishes SSO access to Huawei Cloud, the enterprise user can log in to Huawei Cloud as the IAM user with the specified external identity ID. For example, if an enterprise user **IdP_Test_User** is mapped to the IAM user **Alice**, the enterprise user **IdP_Test_User** will log in to Huawei Cloud as the IAM user **Alice**.

Figure 9-23 Mapping external identities to IAM users



4. **Verify the federated login**: Check whether the enterprise user can log in to Huawei Cloud through SSO.
5. **(Optional) Configure a federated login entry**: Configure the login link (see **Figure 9-24**) in the enterprise IdP to allow enterprise users to be redirected to Huawei Cloud from your enterprise management system.

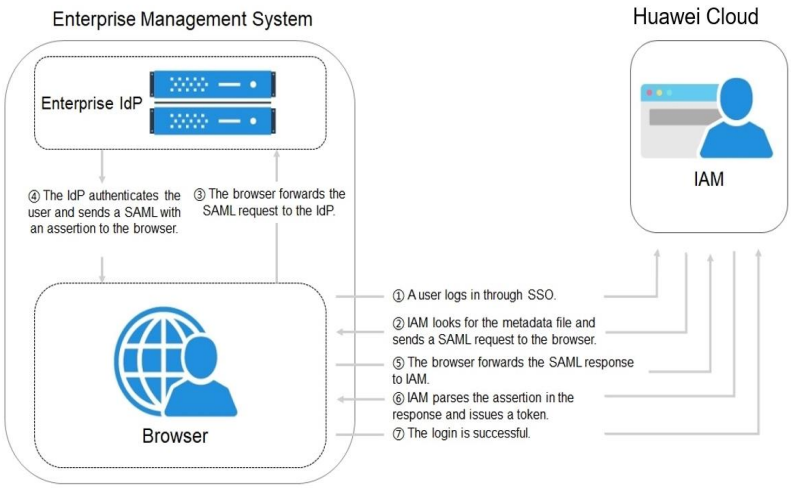
Figure 9-24 SSO login model



How Identity Federation Works

Figure 9-25 shows the identity federation process between an enterprise management system and Huawei Cloud.

Figure 9-25 How identity federation works



NOTE

To view interactive requests and assertions with a better experience, you are advised to use Google Chrome and install SAML Message Decoder.

As shown in **Figure 9-25**, the process of identity federation is as follows:

1. A user opens the login link generated after the IdP creation in the browser. The browser sends an SSO request to Huawei Cloud.
2. Huawei Cloud authenticates the user against the metadata file of the enterprise IdP and constructs a SAML request to the browser.
3. The browser forwards the SAML request to the enterprise IdP.
4. The user enters their username and password on the login page. After the enterprise IdP authenticates the user's identity, it constructs a SAML assertion containing the user details and sends the assertion to the browser as a SAML response.
5. The browser responds and forwards the SAML response to Huawei Cloud.
6. Huawei Cloud parses the assertion in the SAML response, identifies the IAM user group mapping to the user based on the identity conversion rules, and issues a token to the user.
7. The SSO login is successful.

NOTE

The assertion must carry a signature; otherwise, the login will fail.

9.4.2 Creating an IdP Entity

To establish a trust relationship between an enterprise IdP and Huawei Cloud, upload the metadata file of Huawei Cloud to the enterprise IdP, and then create an IdP entity and upload the metadata file of the enterprise IdP on the IAM console.

Establishing a Trust Relationship Between the Enterprise IdP and Huawei Cloud

Configure the metadata file of Huawei Cloud on the enterprise IdP to establish a trust.

Step 1 Download the metadata file of Huawei Cloud.

Visit **https://auth-intl.huaweicloud.com/authui/saml/metadata.xml** (Google Chrome is recommended). Download the Huawei Cloud metadata file and set the file name, for example, **SP-metadata.xml**.

Step 2 Upload the metadata file to the enterprise IdP server. For details, see the help documentation of the enterprise IdP.

Step 3 Obtain the metadata file of the enterprise IdP. For details, see the help documentation of the enterprise IdP.

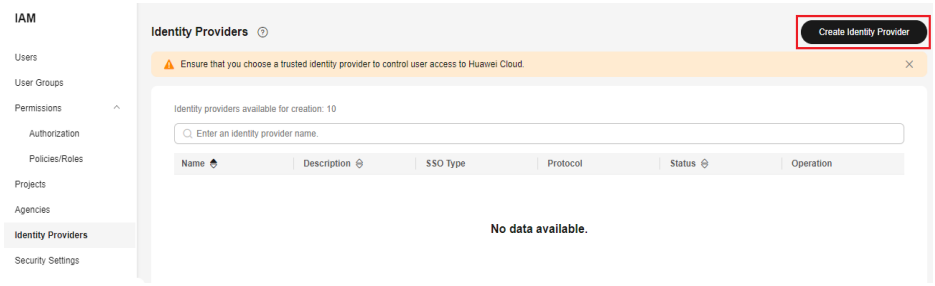
----End

Creating an IdP Entity on Huawei Cloud

To create an IdP entity on the IAM console, do as follows:

Step 1 Log in to the **IAM console**, choose **Identity Providers** from the navigation pane, and click **Create Identity Provider** in the upper right corner.

Figure 9-26 Creating an IdP entity



Step 2 Specify the name, protocol, SSO type, status, and description of the IdP entity.

Figure 9-27 Setting IdP parameters

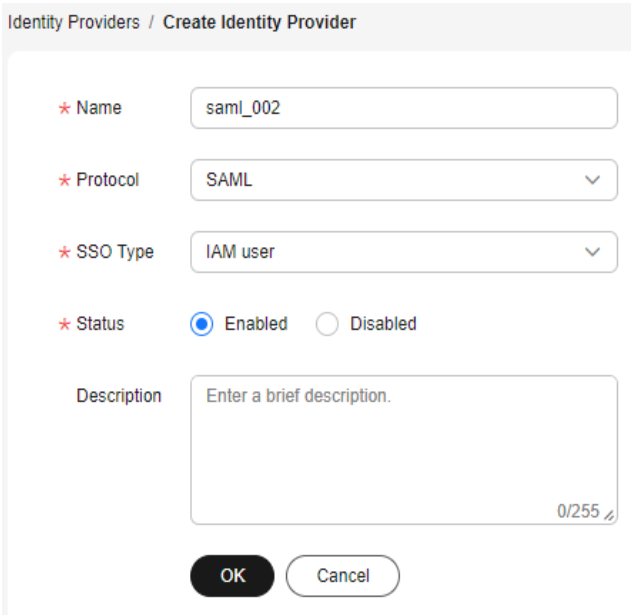


Table 9-6 Basic parameters of an IdP

Parameter	Description
Name	IdP name, which must be unique globally. You are advised to use the domain name.
Protocol	IdP protocol. Huawei Cloud supports SAML and OpenID Connect protocols. For details about OpenID Connect-based identity federation, see **Virtual User SSO via OpenID Connect**.
SSO Type	IdP type. An account can have only one type of IdP. The following describes the IAM user type. IAM user SSO: After a federated user logs in to Huawei Cloud, the system automatically maps the **external identity ID** to an IAM user so that the federated user has the permissions of the mapped IAM user. An account can have only one IdP of the IAM user type. If you select the IAM user SSO, ensure that you have created an IAM user and set the external identity ID. For details, see **Creating an IAM User**.
Status	IdP status. The default value is **Enabled**.

Step 3 Click **OK**.

----End

Configuring the Metadata File of the Enterprise IdP on Huawei Cloud

You can upload the metadata file or manually edit metadata on the IAM console. For a metadata file larger than 500 KB, manually configure the metadata. If the metadata has been changed, upload the latest metadata file or edit the existing

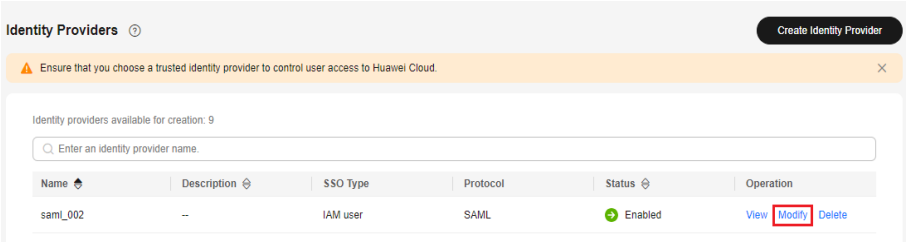
metadata to ensure that the federated users can log in to Huawei Cloud successfully.

NOTE

For details about how to obtain the metadata file of an enterprise IdP, see the help documentation of the enterprise IdP.

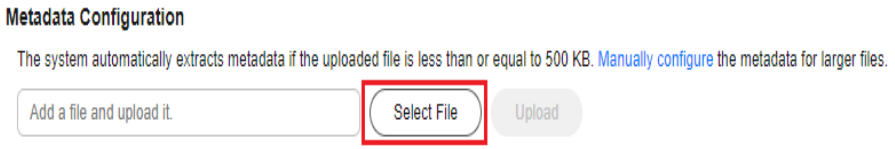
- **Upload a metadata file.**
  a. Click **Modify** in the row containing the IdP.

  Figure 9-28 Modifying an IdP

  b. Click **Select File** and select the metadata file of the enterprise IdP.

  Figure 9-29 Uploading a metadata file

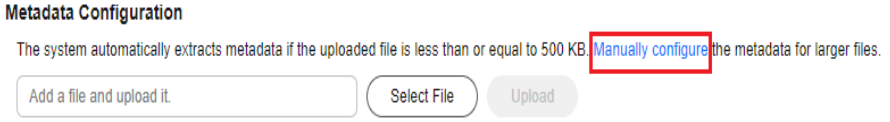
  

  c. Click **Upload**. The metadata extracted from the uploaded file is displayed. Click **OK**.

  - If the uploaded metadata file contains multiple IdPs, select the IdP you want to use from the **Entity ID** drop-down list.
  - If a message is displayed indicating that no entity ID is specified or the signing certificate has expired, check the metadata file and upload it again, or configure the metadata manually.

  d. Click **OK** to save the settings.
- **Manually configure metadata.**
  a. Click **Manually configure**.

  Figure 9-30 Manually configuring metadata

  b. In the **Configure Metadata** dialog box, set the metadata parameters, such as **Entity ID**, **Signing Certificate**, and **SingleSignOnService**.

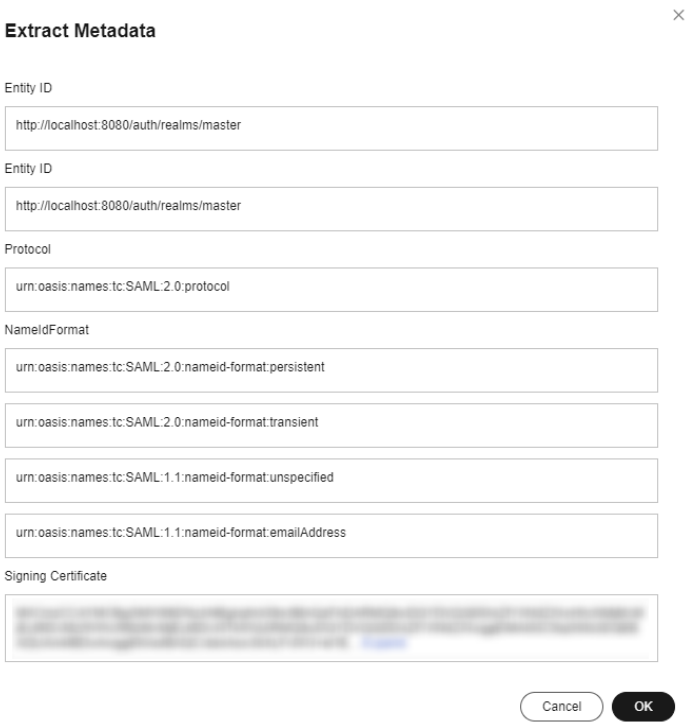
Parameter	Mandatory	Description
Entity ID	Yes	The unique identifier of an IdP. Enter the value of **entityID** displayed in the enterprise IdP's metadata file. If the metadata file contains multiple IdPs, choose the one you want to use.
Protocol	Yes	Protocol used for identity federation between an enterprise IdP and SP. The protocol is selected by default.
NameIdFormat	No	Enter the value of **NameIdFormat** displayed in the IdP metadata file. It specifies the username identifier format supported by the IdP, which is used for communication between the IdP and federated user. If you configure multiple values, Huawei Cloud uses the first value by default.
Signing Certificate	Yes	Enter the value of **<X509Certificate>** displayed in the IdP metadata file. A signing certificate is a public key certificate used for signature verification. For security purposes, enter a public key containing at least 2,048 bits. The signing certificate is used during identity federation to ensure that assertions are credible and complete. If you configure multiple values, Huawei Cloud uses the first value by default.
SingleSignOnService	Yes	Enter the value of **SingleSignOnService** displayed in the IdP metadata file. This parameter defines how SAML requests are sent during SSO. It must support HTTP Redirect or HTTP POST. If you configure multiple values, Huawei Cloud uses the first value by default.
SingleLogoutService	No	Enter the value of **SingleLogoutService** displayed in the IdP metadata file. This parameter indicates the address to which federated users will be redirected after logging out their sessions. It must support HTTP Redirect or HTTP POST. If you configure multiple values, Huawei Cloud uses the first value by default.

The following example shows the metadata file of an enterprise IdP and the manually configured metadata.

Figure 9-31 Metadata file of an enterprise IdP

```
<md:EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:names
:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Name="urn:keycloak">
    <md:EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:nam
es:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="http://localhost:8080/auth/realms/master">
        <md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <md:KeyDescriptor use="signing">
                <ds:KeyInfo>
                    <ds:KeyName>[redacted]</ds:KeyName>
                    <ds:X509Data>
                        <ds:X509Certificate>[redacted]
                        </ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </md:KeyDescriptor>
            <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://localhost:8080/auth/realms/master
/protocol/saml"/>
            <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://localhost:8080/auth/realms/ma
ster/protocol/saml"/>
            <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
            <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
            <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
            <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
            <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://localhost:8080/auth/realms/master
/protocol/saml"/>
            <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://localhost:8080/auth/realms/ma
ster/protocol/saml"/>
            <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="http://localhost:8080/auth/realms/master/prot
ocol/saml"/>
        </md:IDPSSODescriptor>
    </md:EntityDescriptor>
</md:EntitiesDescriptor>
```


Figure 9-32 Manually configuring metadata



c. Click **OK** to save the settings.

9.4.3 Configuring an Enterprise IdP

You can configure parameters in the enterprise IdP to determine what information will be sent to Huawei Cloud. Huawei Cloud authenticates the federated identity and assigns permissions based on the received information.

NOTE

If the SSO type is IAM user, the enterprise IdP must have the **IAM_SAML_Attributes_xUserId** assertion configured.

Common Parameters in an Enterprise IdP

Table 9-7 Common parameters in an enterprise IdP

Parameter	Description	Scenario
IAM_SAML_Attributes_xUserId	ID of an enterprise IdP user (federated user)	This parameter is mandatory when the SSO type is IAM user. Each federated user is mapped to an IAM user. The **IAM_SAML_Attributes_xUserId** of the federated user is the same as the external identity ID of the corresponding IAM user.
IAM_SAML_Attributes_redirect_url	Target URL which the federated user will be redirected to	During SSO login, the federated user will be redirected to a page on Huawei Cloud , for example, the Cloud Eye homepage in the CN-Hong Kong region.
IAM_SAML_Attributes_domain_id	Account ID of Huawei Cloud to be federated with the enterprise IdP	This parameter is mandatory in the enterprise IdP-initiated federation.
IAM_SAML_Attributes_idp_id	Name of the IdP entity created on Huawei Cloud	This parameter is mandatory in the enterprise IdP-initiated federation.

9.4.4 Configuring an External Identity ID

For the IAM user SSO type, you must configure an external identity ID for the IAM user which the federated user maps to on Huawei Cloud. The external identity ID must be the same as the **IAM_SAML_Attributes_xUserId** value of the enterprise IdP user (federated user). You can create an IAM user and configure an external identity ID for it, or change the external identity ID of an existing IAM user.

- **Creating an IAM User and Configuring an External Identity ID**
- **Changing the External Identity ID of an Existing IAM User**

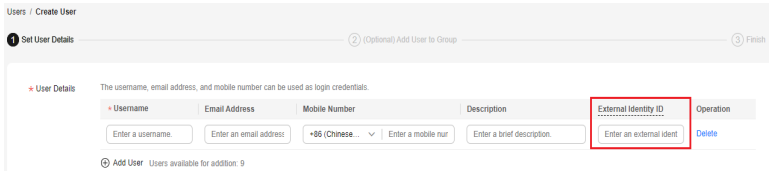
Creating an IAM User and Configuring an External Identity ID

Step 1 Log in to the IAM console as an administrator.

Step 2 On the IAM console, choose **Users** from the navigation pane, and click **Create User** in the upper right corner.

Step 3 In the **User Details** area, configure an external identity ID. For details about other settings, see **Creating an IAM User**.

Figure 9-33 Configuring an external identity ID

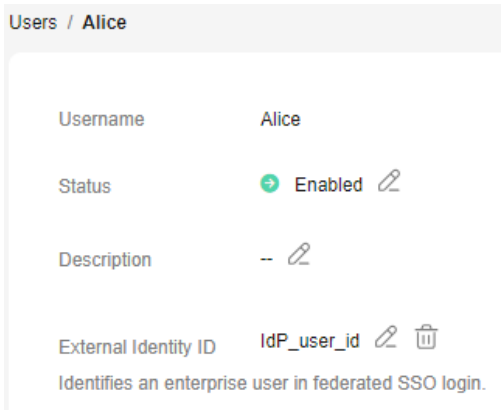


----End

Changing the External Identity ID of an Existing IAM User

In the IAM user list, click a username or choose **More** > **Security Settings** in the row containing the user and change the external identity ID.

Figure 9-34 Changing the external identity ID of an existing IAM user



9.4.5 Verifying the Login

Verifying the Federated Login

Federated users can initiate a login from the IdP or SP.

- Initiating a login from an IdP, for example, Microsoft Active Directory Federation Services (AD FS) or Shibboleth.
- Initiating a login from the SP (Huawei Cloud). You can obtain the login link from the IdP details page on the IAM console.

The IdP-initiated login method depends on the IdP. For details, see the IdP help documentation. This section describes how to initiate a login from the SP.

Step 1 Log in as a federated user.

On the **Identity Providers** page of the IAM console, click **View** in the row containing the IdP. Click to copy the login link displayed in the **Basic Information** area, open the link using a browser, and then enter the username and password used in the enterprise management system.

Figure 9-35 Login link

Step 2 Check whether the federated user is logging in as an IAM user.

----End

Redirecting to a Specified Region or Service

You can specify the target page which the federated user will be redirected to after login, for example, the Cloud Eye homepage in the CN-Hong Kong region.

- Configuring the login link on the SP

  Combine the login link obtained from the console with the specified URL encoded using **UrlEncode**. The combination format is ***Login link*&service=*Specified URL encoded using UrlEncode***. For example, if the login address is **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml** and the destination console address is **https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**, the combined login link is **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml&service=https%3A%2F%2Fconsole-intl.huaweicloud.com%2Fces%2F%3Fregion%3Dap-southeast-1**.
- Configuring the login link on the IdP

  Configure **IAM_SAML_Attributes_redirect_url** (the URL to be redirected to) in the SAML assertion of the enterprise IdP.

9.4.6 Configuring a Federated Login Entry in the Enterprise IdP

Configure a federated login entry in the enterprise IdP so that enterprise users can use the login link to access Huawei Cloud.

NOTE

If you do not want to configure the login entry in your enterprise management system, skip this section. Huawei Cloud provides a login entry for federated users. For details about the login, see **Logging In as a Federated User**.

Prerequisites

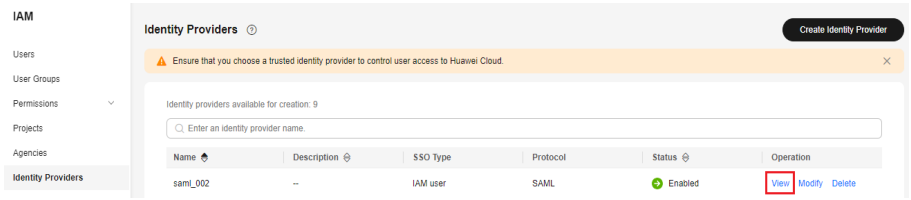
- An IdP entity has been created on Huawei Cloud, and the login link for the IdP is available. For details, see **Creating an IdP Entity**.
- The login entry for logging in to Huawei Cloud has been configured in the enterprise management system.

Procedure

Step 1 Log in to the **IAM console**. In the navigation pane, choose **Identity Providers**.

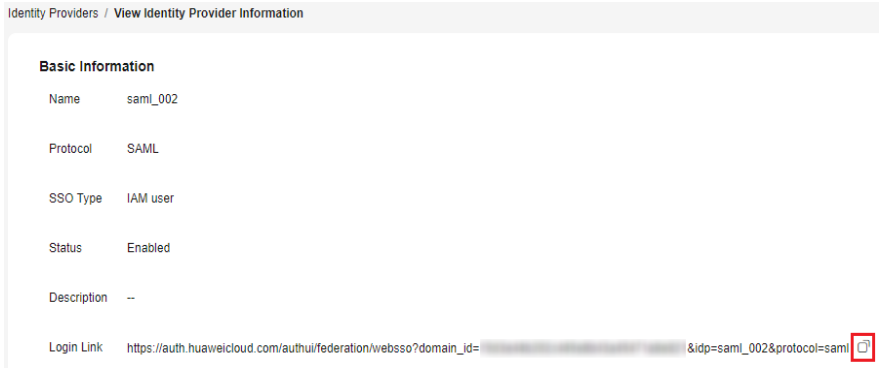
Step 2 Click **View** in the row containing the IdP.

Figure 9-36 Viewing IdP details



Step 3 Copy the login link by clicking in the **Login Link** row.

Figure 9-37 Copying the login link



Step 4 Add the following statement to the page file of the enterprise management system:

```
<a href="<Login link>"> Huawei Cloud login entry </a>
```

Step 5 Log in to the enterprise management system using your enterprise account, and click the configured login link to access Huawei Cloud.

----End

9.5 Virtual User SSO via OpenID Connect

9.5.1 Overview of Virtual User SSO via OpenID Connect

This section describes how to configure identity federation and how identity federation works.

Configuring Identity Federation

The following describes how to configure your enterprise IdP and Huawei Cloud to trust each other.

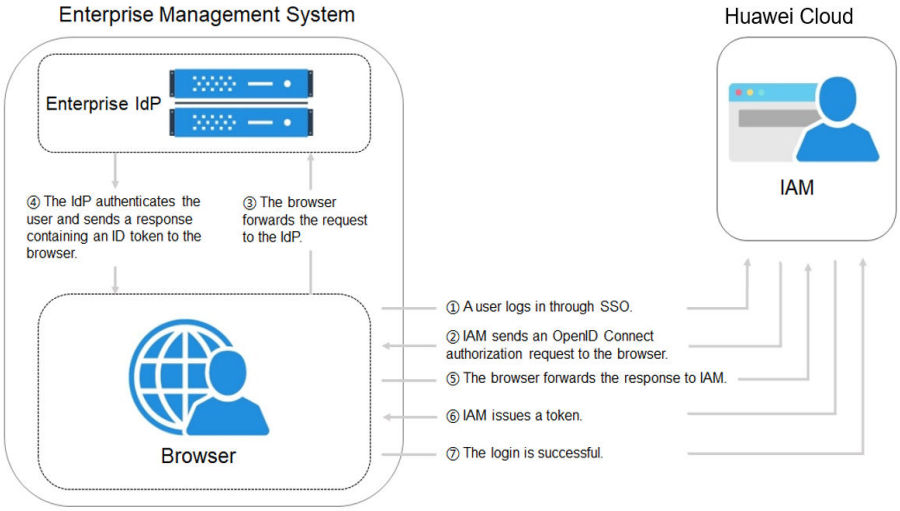
1. **Create an IdP entity and establish a trust relationship**: Create OAuth 2.0 credentials in the enterprise IdP. On Huawei Cloud, create an IdP entity and establish a trust relationship between the two systems.

2. **Configure identity conversion rules**: Configure identity conversion rules on Huawei Cloud to map the users, user groups, and permissions in the enterprise IdP to Huawei Cloud.
3. **Configure a federated login entry**: Configure the login link in the enterprise IdP to allow enterprise users to be redirected to Huawei Cloud from your enterprise management system.

How Identity Federation Works

Figure 9-38 shows the identity federation process between an enterprise management system and Huawei Cloud.

Figure 9-38 How identity federation works



The process of identity federation is as follows:

1. A user opens the login link obtained from the IAM console in the browser. The browser sends an SSO request to Huawei Cloud.
2. Huawei Cloud authenticates the user against the configuration of the enterprise IdP and constructs an OpenID Connect request to the browser.
3. The browser forwards the OpenID Connect request to the enterprise IdP.
4. The user enters their username and password on the login page displayed in the enterprise IdP. After the enterprise IdP authenticates the user's identity, it constructs an ID token containing the user information, and sends the ID token to the browser as an OpenID Connect authorization response.
5. The browser responds and forwards the OpenID Connect response to Huawei Cloud.
6. Huawei Cloud parses the ID token in the OpenID Connect response, identifies the IAM user group mapping to the user based on the identity conversion rules, and issues a token to the user.
7. The SSO login is successful.

9.5.2 Creating an IdP Entity

To establish a trust relationship between an enterprise IdP and Huawei Cloud, set the user redirect URLs and create OAuth 2.0 credentials in the enterprise IdP. On the IAM console, create an IdP entity and configure authorization information.

Prerequisites

- The enterprise administrator has created an account in Huawei Cloud, and has created user groups and assigned them permissions in IAM. For details, see **Creating a User Group and Assigning Permissions**. The user groups created in IAM will be mapped to federated users so that the federated users can obtain the permissions of the user groups to use Huawei Cloud resources.
- The enterprise administrator has read the help documentation of the enterprise IdP or has understood how to use the enterprise IdP. Configurations of different enterprise IdPs differ greatly, so they are not described in this document. For details about how to obtain an enterprise IdP's OAuth 2.0 credentials, see the IdP help documentation.

Creating OAuth 2.0 Credentials in the Enterprise IdP

Step 1 Set redirect URIs **https://auth.huaweicloud.com/authui/oidc/redirect** and **https://auth.huaweicloud.com/authui/oidc/post** in the enterprise IdP so that users can be redirected to the OpenID Connect IdP in Huawei Cloud.

Step 2 Obtain OAuth 2.0 credentials of the enterprise IdP.

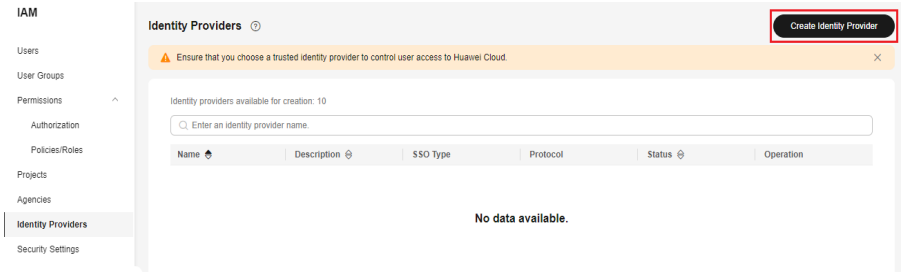
----End

Creating an IdP Entity on Huawei Cloud

Create an IdP entity and configure authorization information in IAM to establish a trust relationship between the enterprise IdP and IAM.

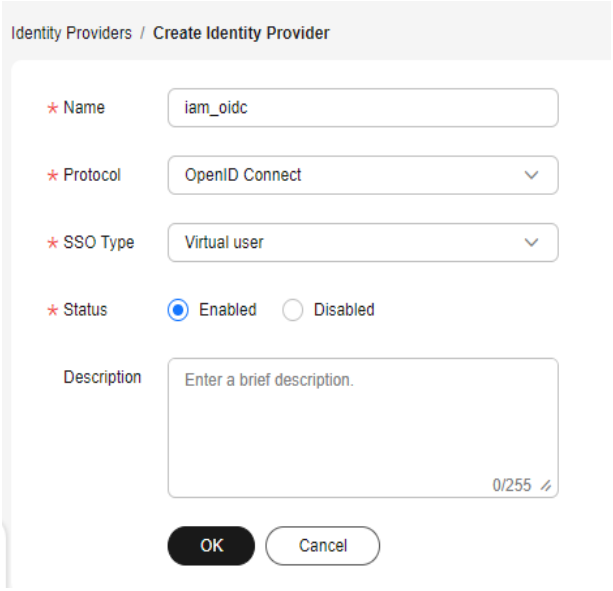
Step 1 Log in to the **IAM console**, choose **Identity Providers** from the navigation pane, and click **Create Identity Provider** in the upper right corner.

Figure 9-39 Creating an IdP entity



Step 2 Enter an IdP name, select **OpenID Connect** and **Enabled**, and click **OK**.

Figure 9-40 Setting IdP parameters



NOTE

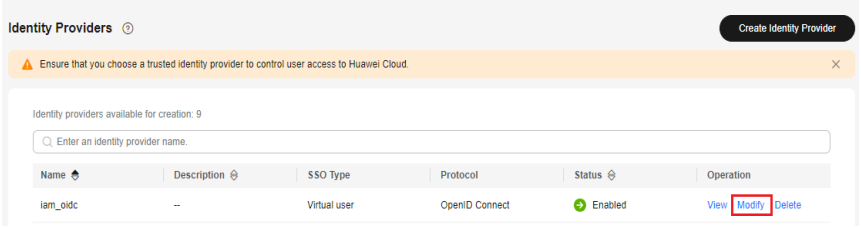
The IdP name must be unique under your account. You are advised to use the domain name.

----End

Configuring Authorization Information in Huawei Cloud

Step 1 Click **Modify** in the **Operation** column of the row containing the IdP you want to modify.

Figure 9-41 Modifying an IdP



Step 2 Select an access type.

Figure 9-42 Access type

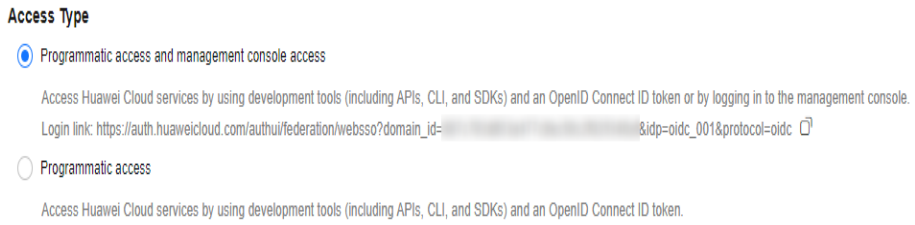


Table 9-8 Access type description

Access Type	Description
Programmatic access and management console access	• Programmatic access: Federated users can use development tools (including APIs, CLI, and SDKs) that support key authentication to access Huawei Cloud. • Management console access: Federated users can log in to Huawei Cloud by using their own usernames and passwords. Select this access type if you want users to access Huawei Cloud through SSO.
Programmatic access	Federated users can only use development tools (including APIs, CLI, and SDKs) that support key authentication to access Huawei Cloud.

Step 3 Specify the configuration information.

Table 9-9 Configuration information

Parameter	Description
Identity Provider URL	URL of the OpenID Connect IdP. Set it to the value of **issuer** in the **Openid-configuration**. **NOTE** **Openid-configuration** indicates a URL defined in OpenID Connect, containing configurations of an enterprise IdP. The URL format is **https://***{base URL}***/.well-known/openid-configuration**, where *base URL* is defined by the enterprise IdP. For example, the **Openid-configuration** of Google is **https://accounts.google.com/.well-known/openid-configuration**.
Client ID	ID of a client registered with the OpenID Connect IdP. The client ID is **an OAuth 2.0 credential created in the enterprise IdP**.
Authorization Endpoint	Authorization endpoint of the OpenID Connect IdP. Set it to the value of **authorization_endpoint** in **Openid-configuration**. This parameter is required only if you set **Access Type** to **Programmatic access and management console access**.
Scopes	Scopes of authorization requests. **openid** is selected by default. This parameter is required only if you set **Access Type** to **Programmatic access and management console access**. Enumerated values: • openid • email • profile

Parameter	Description
Response Type	Response type of authorization requests. The default value is **id_token**. This parameter is required only if you set **Access Type** to **Programmatic access and management console access**.
Response Mode	Response mode of authorization requests. The options include **form_post** and **fragment**. **form_post** is recommended. • **form_post**: If this mode is selected, set the redirect URL to **https://auth.huaweicloud.com/authui/oidc/post** in the enterprise IdP. • **fragment**: If this mode is selected, set the redirect URL to **https://auth.huaweicloud.com/authui/oidc/redirect** in the enterprise IdP. This parameter is required only if you set **Access Type** to **Programmatic access and management console access**.
Signing Key	Public key used to sign the ID token of the OpenID Connect IdP. For account security purposes, change the signing key periodically.

Step 4 Click **OK**.

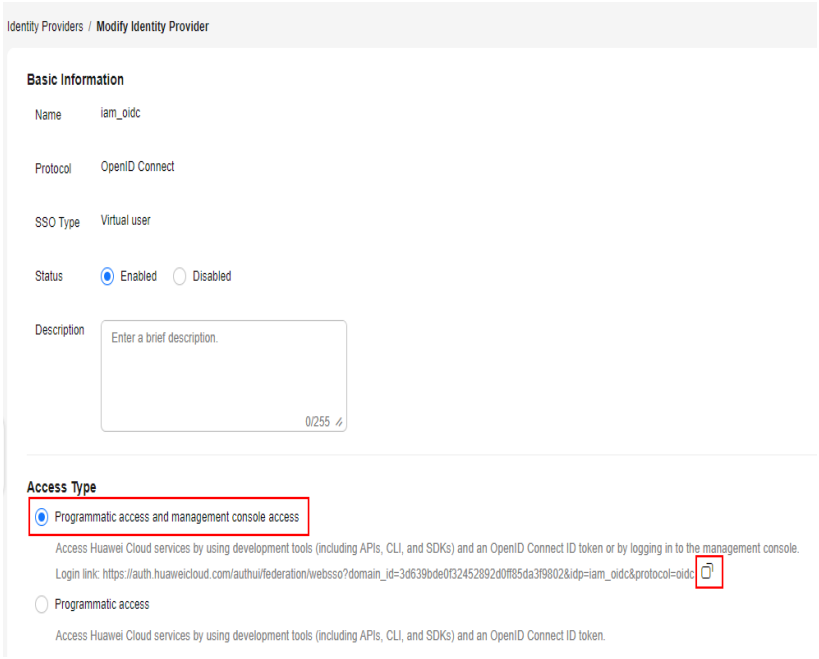
----End

Verifying the Federated Login

Step 1 Click the login link displayed on the IdP details page and check if the login page of the enterprise IdP server is displayed.

1. On the **Identity Providers** page, click **Modify** in the **Operation** column of the identity provider.
2. Copy the login link displayed on the **Modify Identity Provider** page and visit the link using a browser.

Figure 9-43 Copying the login link



3. If the enterprise IdP login page is not displayed, check the configurations of the IdP and the enterprise IdP server.

Step 2 Enter the username and password of a user that was created in the enterprise management system.

- If the login is successful, add the login link to the enterprise management system.
- If the login fails, check the username and password.

NOTE

Federated users can only access Huawei Cloud by default. To assign permissions to federated users, configure identity conversion rules for the IdP. For details, see **Configuring Identity Conversion Rules**.

----End

Related Operations

- Viewing IdP information: In the IdP list, click **View** in the row containing the IdP, and view its basic information, metadata, and identity conversion rules.

  NOTE

  To modify the configuration of an IdP, click **Modify** at the bottom of the details page.

- Modifying an IdP: In the IdP list, click **Modify** in the row containing the IdP, and then change its status or modify the description, metadata, or identity conversion rules.
- Deleting an IdP: In the IdP list, click **Delete** in the row containing the IdP, and click **OK** in the displayed dialog box.

Follow-Up Procedure

- Configure identity conversion rules to map enterprise IdP users to IAM user groups and assign permissions to the users. For details, see **Configuring Identity Conversion Rules**.
- Configure the enterprise management system to allow users to access Huawei Cloud through SSO. For details, see **Configuring a Federated Login Entry in the Enterprise IdP**.

9.5.3 Configuring Identity Conversion Rules

Federated users are named **FederationUser** by default in Huawei Cloud. These users can only log in to Huawei Cloud and they do not have any other permissions. You can configure identity conversion rules on the IAM console to achieve the following:

- Display enterprise users with different names in Huawei Cloud.
- Assign permissions to enterprise users to use Huawei Cloud resources by mapping these users to IAM user groups. Ensure that you have created the required user groups. For details, see **Creating a User Group and Assigning Permissions**.

NOTE

- Modifications to identity conversion rules will take effect the next time federated users log in.
- To modify the permissions of a user, modify the permissions of the user group which the user belongs to. Then restart the enterprise IdP for the modifications to take effect.

Prerequisites

An IdP entity has been created, and the login link of the IdP is accessible. (For details about how to create and verify an IdP entity, see **Creating an IdP Entity**.)

Procedure

If you configure identity conversion rules by clicking **Create Rule**, IAM converts the rule parameters to the JSON format. Alternatively, you can click **Edit Rule** to configure rules in JSON format. For details, see **Syntax of Identity Conversion Rules**.

- **Creating Rules**
  a. Log in to the **IAM console** as the administrator. In the navigation pane, choose **Identity Providers**.
  b. In the IdP list, click **Modify** in the row containing the IdP.
  c. In the **Identity Conversion Rules** area, click **Create Rule**. Then, configure the rules in the **Create Rule** dialog box.

Figure 9-44 Creating rules

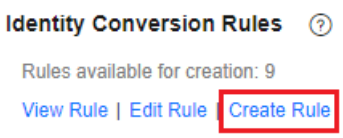


Figure 9-45 Creating rules

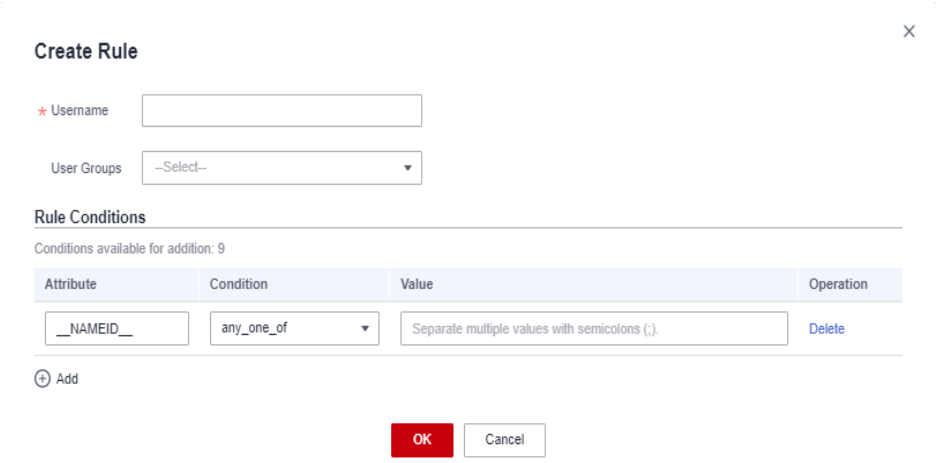


Table 9-10 Parameter description

Parameter	Description	Remarks
Username	Username of federated users in Huawei Cloud.	To distinguish federated users from Huawei Cloud users, it is recommended that you set the username to **FederationUser-***IdP_XXX*. *IdP* indicates an IdP name, for example, AD FS or Shibboleth. *XXX* indicates a custom name. **NOTICE** • The username of each federated user must be unique in the same IdP. Federated users with the same usernames in the same IdP will be mapped to the same IAM user in Huawei Cloud. • The username can only contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.). It cannot start with a digit and cannot contain the following special characters: ", \", \\, \n, \r
User Groups	User groups which the federated users belong to in Huawei Cloud.	The federated users will inherit permissions from their user groups. You can select a user group that has already been created.

Parameter	Description	Remarks
Rule Conditions	Conditions that a federated user must meet to obtain permissions from the selected user groups.	Federated users who do not meet these conditions cannot access Huawei Cloud. You can create a maximum of 10 conditions for an identity conversion rule. **NOTE** • An identity conversion rule can have multiple conditions. It takes effect only if all of the conditions are met. • An IdP can have multiple identity conversion rules. If a federated user does not meet any of the conditions, the user will be denied to access Huawei Cloud.

For example, set an identity conversion rule for administrators in the enterprise management system.

- Username: **FederationUser-IdP_admin**
- User group: **admin**
- Rule condition: **_NAMEID_** (attribute), **any_one_of** (condition), and **000000001** (value).

  Only the user with ID 000000001 is mapped to IAM user **FederationUser-IdP_admin** and inherits permissions from the **admin** user group.

d. In the **Create Rule** dialog box, click **OK**.

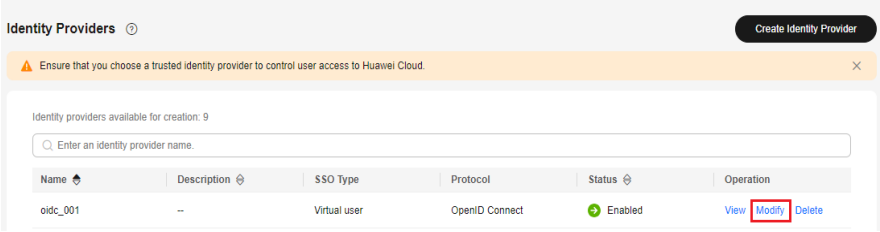
e. On the **Modify Identity Provider** page, click **OK**.

- **Editing Rules**

a. Log in to the **IAM console** as the administrator. In the navigation pane, choose **Identity Providers**.

b. In the IdP list, click **Modify** in the row containing the IdP.

Figure 9-46 Modifying an IdP



c. In the **Identity Conversion Rules** area, click **Edit Rule**.

d. Edit the identity conversion rules in JSON format. For details, see **Syntax of Identity Conversion Rules**.

e. Click **Validate** to verify the syntax of the rules.

f. If the rule is correct, click **OK** in the **Edit Rule** dialog box, and click **OK** on the **Modify Identity Provider** page.

If a message indicating that the JSON file is incomplete is displayed, modify the statements or click **Cancel** to cancel the modifications.

Verifying Federated User Permissions

After configuring identity conversion rules, verify the permissions of federated users.

Step 1 Log in as a federated user.

On the **Identity Providers** page of the IAM console, click **View** in the row containing the IdP. Click to copy the login link displayed in the **Basic Information** area, open the link using a browser, and then enter the username and password used in the enterprise management system.

Step 2 Check that the federated user has the permissions assigned to their user group.

For example, configure an identity conversion rule to map federated user **ID1** to the **admin** user group so that **ID1** will have full permissions for all cloud services. On the management console, select a cloud service, and check if you can access the service.

----End

Related Operations

Viewing identity conversion rules: Click **View Rule** on the **Modify Identity Provider** page. The identity conversion rules are displayed in JSON format. For details about the JSON format, see **Syntax of Identity Conversion Rules**.

9.5.4 Configuring a Federated Login Entry in the Enterprise IdP

Configure a federated login entry in the enterprise IdP so that enterprise users can use the login link to access Huawei Cloud.

NOTE

If no login link has been configured in your enterprise management system, federated users in your enterprise can log in to Huawei Cloud through the Huawei Cloud login page. For details, see **Logging In as a Federated User**.

Prerequisites

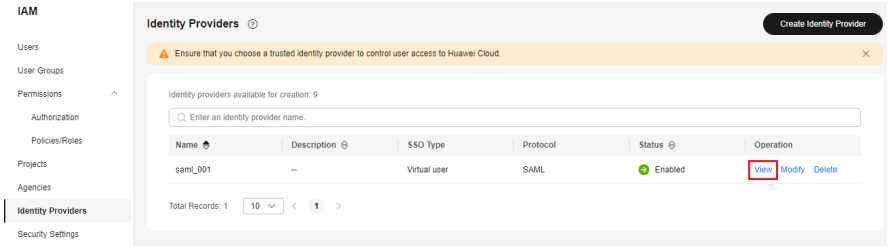
- An IdP entity has been created on Huawei Cloud. For details about how to create an IdP entity, see **Creating an IdP Entity**.
- The login entry for logging in to Huawei Cloud has been configured in the enterprise management system.

Procedure

Step 1 Log in to the **IAM console**. In the navigation pane, choose **Identity Providers**.

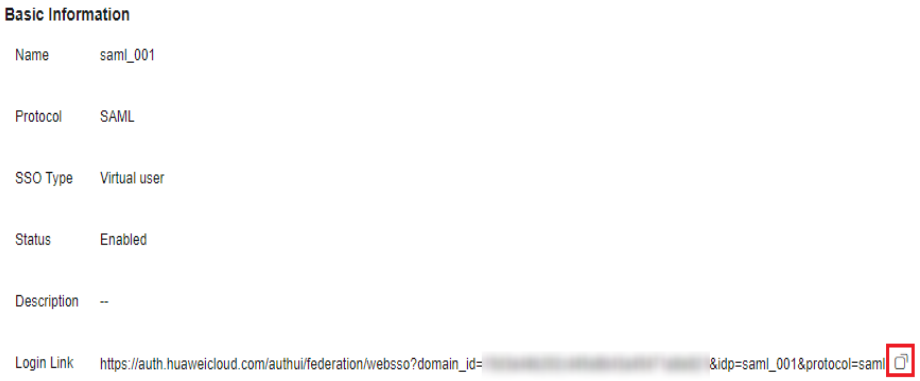
Step 2 Click **View** in the row containing the IdP.

Figure 9-47 Viewing IdP details



Step 3 Copy the login link by clicking in the **Login Link** row.

Figure 9-48 Copying the login link



Step 4 Add the following statement to the page file of the enterprise management system:

```
<a href="<Login link>"> Huawei Cloud login entry </a>
```

Step 5 Log in to the enterprise management system using your enterprise account, and click the configured login link to access Huawei Cloud.

----End

9.6 Syntax of Identity Conversion Rules

An identity conversion rule is a JSON object which can be modified. The following is an example JSON object:

```
[
	{
		"local": [
			{
				"<user> or <group> or <groups>"
			}
		],
		"remote": [
			{
				"<condition>"
			}
		]
	}
]
```

Parameter description:

- **local**: Identity information of a federated user mapped to IAM. The value of this field can contain placeholders, such as **{0...n}**. The attributes **{0}** and **{1}** represent the first and second remote attributes of the user information, respectively.
- **remote**: Information about a federated user of the IdP. This field is an expression consisting of assertion attributes and operators. The value of this field is determined by the assertion.
  - **condition**: Conditions for the identity conversion rule to take effect. The following three types of conditions are supported:
    - **empty**: The rule is matched to all claims containing the attribute type. This condition does not need to be specified. The condition result is the argument that is passed as input.
    - **any_one_of**: The rule is matched only if any of the specified strings appear in the attribute type. The condition result is Boolean, not the argument that is passed as input.
    - **not_any_of**: The rule is not matched if any of the specified strings appear in the attribute type. The condition result is Boolean, not the argument that is passed as input.

NOTICE

The user information mapped to IAM can only contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.), and cannot start with a digit.

Examples of the Empty Condition

The **empty** condition returns character strings to replace the local attributes **{0..n}**.

- In the following example, the username of the federated user is "the first remote attribute value+space+the second remote attribute value" in IAM, that is, *FirstName LastName*. The group that the user belongs to is the third remote attribute value, that is, *Group*. The Group attribute has only one value.

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0} {1}"
                }
            },
            {
                "group": {
                    "name": "{2}"
                }
            }
        ],
        "remote": [
            {
                "type": "FirstName"
            },
            {
                "type": "LastName"
            },
```



```
            {
               "type": "Group"
            }
         ]
      }
]
```

The following assertion (simplified for easy understanding) indicates that the username of the federated user is **John Smith** and the user only belongs to the **admin** group.

```
{FirstName: John}
{LastName: Smith}
{Group: admin}
```

- If a federated user belongs to multiple user groups in IAM, the identity conversion rule can be configured as follows.

  In the following example, the username of the federated user is "the first remote attribute value+space+the second remote attribute value" in IAM, that is, *FirstName LastName*. The groups that the user belongs to are the third remote attribute value, that is, *Groups*.

```
[
      {
         "local": [
            {
               "user": {
                  "name": "{0} {1}"
               }
            },
            {
               "group":   {
                  "name": "{2}"
               }
            }
         ],
         "remote": [
            {
               "type": "FirstName"
            },
            {
               "type": "LastName"
            },
            {
               "type": "Groups"
            }
         ]
      }
]
```

  The following assertion indicates that the username of the federated user is **John Smith** and the user belongs to the **admin** and **manager** groups.

```
{FirstName: John}
{LastName: Smith}
{Groups: [admin, manager]}
```

Examples of the "any one of" and "not any of" Conditions

Unlike the **empty** condition, the **any one of** and **not any of** conditions return Boolean values. These values will not be used to replace the local attributes. In the following example, only **{0}** is replaced by the returned value of the first **empty** condition in the **remote** block. The value of **group** is fixed as **admin**.

- The username of the federated user in IAM is the first remote attribute value, that is, *UserName*. The federated user belongs to the **admin** group. This rule

takes effect only for users who are members of the **idp_admin** group in the IdP.

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            },
            {
                "group": {
                    "name": "admin"
                }
            }
        ],
        "remote": [
            {
            "type": "UserName"
            },
            {
                "type": "Groups",
                "any_one_of": [
                    "idp_admin"
                ]
            }
        ]
    }
]
```

- If a federated user belongs to multiple user groups in IAM, the identity conversion rule can be configured as follows.

  The username of the federated user in IAM is the first remote attribute value, that is, *UserName*. The federated user belongs to the **admin** and **manager** groups. This rule takes effect only for users who are members of the **idp_admin** group in the IdP.

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            },
            {
                "group": {
                      "name":"admin"
                }
            },
            {
                "group": {
                      "name":"manager"
                }
            }
        ],
        "remote": [
            {
            "type": "UserName"
            },
            {
                "type": "Groups",
                "any_one_of": [
                    "idp_admin"
                ]
            }
        ]
```



```
        }
    ]
```

- The following assertion indicates that the federated user John Smith is a member of the **idp_admin** group. Therefore, the user can access Huawei Cloud.

  ```
  {UserName: John Smith}
  {Groups: [idp_user, idp_admin, idp_agency]}
  ```

- The following assertion indicates that the federated user John Smith is not a member of the **idp_admin** group. Therefore, the rule does not take effect for the user and the user cannot access Huawei Cloud.

  ```
  {UserName: John Smith}
  {Groups: [idp_user, idp_agency]}
  ```

Example Condition Containing a Regular Expression

You can add **"regex": true** to a condition to calculate results using a regular expression.

This rule takes effect for any user whose username ends with **@mail.com**. The username of each applicable federated user is *UserName* in IAM and the user belongs to the **admin** group.

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            },
            {
                "group": {
                    "name": "admin"
                }
            }
        ],
        "remote": [
            {
            "type": "UserName"
            },
            {
                "type": "Groups",
                "any_one_of": [
                    ".*@mail.com$"
                ],
                "regex": true
            }
        ]
    }
]
```

Examples of Combined Conditions

Multiple conditions can be combined using the logical operator AND.

This rule takes effect only for the federated users who do not belong to the **idp_user** or **idp_agent** user group in the IdP. The username of each applicable federated user is *UserName* in IAM and the user belongs to the **admin** group.

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
```



```
            }
         },
         {
            "group": {
               "name": "admin"
            }
         }
      ],
      "remote": [
         {
         "type": "UserName"
         },
         {
            "type": "Groups",
            "not_any_of": [
               "idp_user"
            ]
         },
         {
            "type": "Groups",
            "not_any_of": [
               "idp_agent"
            ]
         }
      ]
   }
]
```

The preceding rule is equivalent to the following:

```
[
   {
      "local": [
         {
            "user": {
               "name": "{0}"
            }
         },
         {
            "group": {
               "name": "admin"
            }
         }
      ],
      "remote": [
         {
         "type": "UserName"
         },
         {
            "type": "Groups",
            "not_any_of": [
               "idp_user",
               "idp_agent"
            ]
         }
      ]
   }
]
```

Examples of Combined Rules

If multiple rules are combined, the methods for matching usernames and user groups are different.

The username of the federated user is the username matched in the first rule that takes effect. A federated user can log in to Huawei Cloud only if there is at least one rule taking effect to match the username. The user belongs to all groups

matched in all rules that take effect. For easy understanding, username and user group rules can be configured separately.

In the following example, the rules take effect for users in the **idp_admin** group. The username of each applicable federated user is *UserName* in IAM and the user belongs to the **admin** group.

```
[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      }
    ],
    "remote": [
      {
        "type": "UserName"
      }
    ]
  },
  {
    "local": [
      {
        "group": {
          "name": "admin"
        }
      }
    ],
    "remote": [
      {
        "type": "Groups",
        "any_one_of": [
          "idp_admin"
        ]
      }
    ]
  }
]
```

The following assertion indicates that user John Smith is a member of the **idp_admin** group in the IdP and therefore meets the rules. The username of this user is **John Smith** in IAM, and the user belongs to the **admin** group.

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```


10 Custom Identity Broker

10.1 Configuring a Custom Identity Broker with an Agency

If the **IdP of your enterprise** is not compatible with SAML or OpenID Connect, you can create a custom identity broker to enable access to Huawei Cloud. You can write and run code to generate a login URL. Users in your enterprise can then use the URL to log in to Huawei Cloud. The users will be authenticated by your enterprise IdP.

NOTE

If your enterprise IdP is compatible with SAML or OpenID Connect, configure **identity federation** to enable users in your enterprise to access Huawei Cloud through SSO.

Prerequisites

- Your enterprise has an enterprise management system.
- You have registered an account (for example, **DomainA**) in Huawei Cloud as an enterprise administrator and has created a user group (for example, **GroupC**) and assigned it the **Agent Operator** role. (For details, see **Creating a User Group and Assigning Permissions**.)

Procedure

Step 1 Use the **DomainA** account to create an IAM user (for example, **UserB**) and add the user to **GroupC** by following the instructions in **Adding Users to a User Group**.

NOTE

Ensure that the IAM user can **programmatically access** Huawei Cloud services. For details about how to change the access type, see **Managing IAM User Information**.

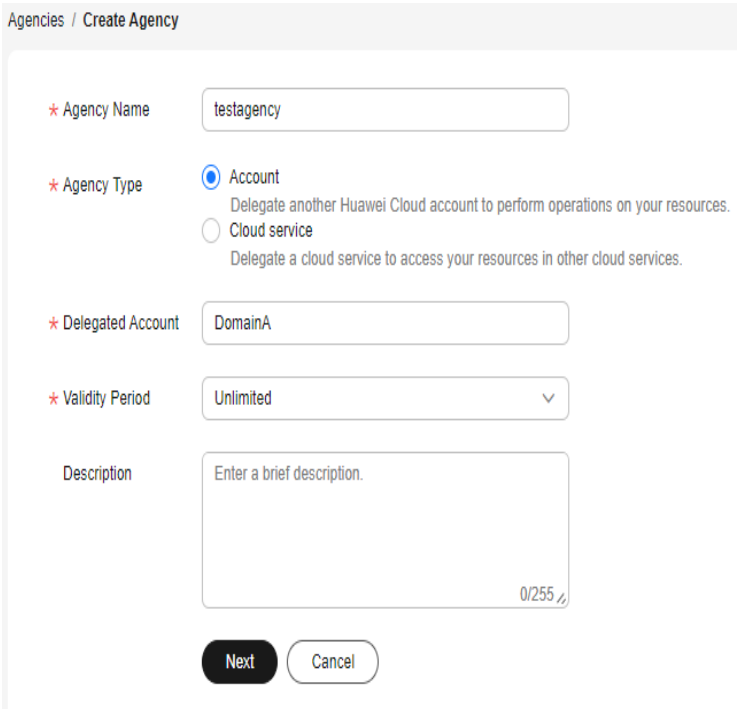
Step 2 Configure the **access key** (recommended) or username and password of **UserB** in the configuration file of your enterprise IdP so that the user can obtain a token for calling APIs. For account security, encrypt the password and access keys before you store them.

Step 3 In the navigation pane of the IAM console, choose **Agencies**. Then, click **Create Agency** in the upper right corner.

Step 4 Set agency parameters.

For example, set the agency name to **testagency**, agency type to **Account**, and delegated account to **DomainA**. Set the validity period and click **Next**.

Figure 10-1 Creating an agency



Step 5 Set the authorization scope, and select the permissions you want to grant to the agency.

Step 6 In the enterprise IdP, create a user group named **testagency** (same as the name of the agency created in **Step 4**), add enterprise users to the group, and grant the users permissions to log in to Huawei Cloud through a custom identity broker. For details, see the documentation of the enterprise IdP.

Step 7 After an enterprise user logs in to the enterprise management system, the user can access the custom identity broker of the enterprise IdP by selecting an agency from the agency list. The user can obtain the agency from the security administrator or root user. For details, see the documentation of the enterprise management system.

NOTE

The agencies of the identity broker must exist in Huawei Cloud and have the same names as some user groups created in the enterprise IdP.

Step 8 The custom identity broker uses the token of **userB** to call the API **POST /v3.0/OS-CREDENTIAL/securitytokens** used to obtain a temporary security token. For details, see **Obtaining a Temporary Access Key and Security Token Through an Agency**.

NOTE

When obtaining a security token with an agency, set the **session_user.name** parameter in the request body.

Step 9 The custom identity broker uses the temporary access key, security token, and global domain name of IAM (**iam.myhuaweicloud.com**) to call the API **POST /v3.0/OS-AUTH/securitytoken/logintokens** for obtaining a login token. The value of **X-Subject-LoginToken** in the response header is a login token. For details, see **Obtaining a Login Token**.

NOTE

- To obtain a login token by calling the API **POST /v3.0/OS-AUTH/securitytoken/logintokens**, use the global domain name (**iam.myhuaweicloud.com**) of IAM.
- A login token is issued to a user to log in through a custom identity broker and contains identity and session information about the user. A login token is valid for 10 minutes by default. Login tokens are required for authentication when users log in to a service console using the FederationProxyUrl.
- You can set the validity period of a login token by calling the API **POST /v3.0/OS-AUTH/securitytoken/logintokens**. The validity period ranges from 10 minutes to 12 hours. If the value you have specified is greater than the remaining validity period of the temporary security token, the remaining validity period of the temporary security token is used.

Step 10 The custom identity broker generates a FederationProxyUrl and returns it to the browser through **Location**. The FederationProxyUrl will be in the following format:

https://auth.huaweicloud.com/authui/federation/login?idp_login_url={enterprise_system_loginURL}&service={console_service_region_url}*&logintoken={logintoken}*

Example:

*https://auth.huaweicloud.com/authui/federation/login?idp_login_url=https%3A%2F%2Fexample.com&service=https%3a%2f%2fconsole.huaweicloud.com%2fapm%2f%3fregion%3dcn-north-4%23%2fapm%2fatps%2ftopology&logintoken=******

Table 10-1 Parameter description

Parameter	Description
idp_login_url	Login URL of the enterprise management system.
service	Access address of a Huawei Cloud service.
logintoken	Login token of the custom identity broker.

The preceding three parameters must be encoded using URLEncode to ensure that they can be identified by the browser.

For details about how to create a FederationProxyUrl, view the example provided in **Creating a FederationProxyUrl Using an Agency**.

NOTE

The FederationProxyUrl contains the login token that has been obtained from IAM, and must be encoded using UrlEncode.

Step 11 If the login token is authenticated successfully, federated users will be automatically redirected to the Huawei Cloud service address specified in the **service** parameter.

If the login token fails to be authenticated, federated users will be redirected to the address specified in **idp_login_url**.

----End

10.2 Creating a FederationProxyUrl Using an Agency

This section provides example code used to programmatically create a FederationProxyUrl using an agency for logging in to Huawei Cloud services.

Example Code Using Java

The following Java code shows how to create a FederationProxyUrl that gives federated users direct access to the Huawei Cloud console.

```
import java.net.*;
import java.util.Collections;
import com.huaweicloud.sdk.core.auth.GlobalCredentials;
import com.huaweicloud.sdk.core.exception.ClientRequestException;
import com.huaweicloud.sdk.core.exception.ServerResponseException;
import com.huaweicloud.sdk.core.http.HttpConfig;
import com.huaweicloud.sdk.iam.v3.IamClient;
import com.huaweicloud.sdk.iam.v3.model.*;


// Use the global domain name to obtain a login token.
String endpoint = "https://iam.myhuaweicloud.com";

// Configure client attributes.
HttpConfig config = HttpConfig.getDefaultHttpConfig()
        .withIgnoreSSLVerification(true)
        .withProxyHost("proxy.huawei.com")
        .withProxyPort(8080);

// Use the domain ID (account ID), AK, and SK of userB to initialize the specified IAM client
"{Service}Client". For details about how to create userB, see section "Creating an IAM User".
IamClient iamClient = IamClient.newBuilder().withCredential(new GlobalCredentials()
        .withDomainId("domainId")
        .withAk("ak")
        .withSk("sk"))
        .withEndpoint(endpoint)
        .withHttpConfig(config)
        .build();

/*CreateTemporaryAccessKeyByAgency
Call the API used to obtain a temporary access key and security token with an agency.
The default validity period of an access key and security token is 900 seconds, that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this example, the validity period is set to 3600 seconds, that is, 1 hour.
When you obtain a login token with a specified validity period, ensure that the validity period of the login token is not greater than the remaining validity period of the security token.
*/
IdentityAssumerole identityAssumerole = new IdentityAssumerole().
        withAgencyName("testagency").withDomainId("0525e2c87exxxxxxx").withSessionUser(new
```

```
AssumeroleSessionuser().withName("ExternalUser")).withDurationSeconds(3600);
AgencyAuth agencyAuth = new AgencyAuth().withIdentity(new
AgencyAuthIdentity().withAssumeRole(identityAssumerole).

withMethods(Collections.singletonList(AgencyAuthIdentity.MethodsEnum.fromValue("assume_role"))));
CreateTemporaryAccessKeyByAgencyRequestBody createTemporaryAccessKeyByAgencyRequestBody = new
CreateTemporaryAccessKeyByAgencyRequestBody().withAuth(agencyAuth);
CreateTemporaryAccessKeyByAgencyResponse createTemporaryAccessKeyByAgencyResponse =
iamClient.createTemporaryAccessKeyByAgency(new
CreateTemporaryAccessKeyByAgencyRequest().withBody(createTemporaryAccessKeyByAgencyRequestBody));
Credential credential = createTemporaryAccessKeyByAgencyResponse.getCredential();

/*CreateLoginToken
Obtain a login token.
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 default validity period of a login token is 600 seconds, that is, 10 minutes. The value ranges from 10
minutes to 12 hours. In this example, the validity period is set to 1800 seconds, that is, half an hour.
Ensure that the validity period of the login token is not greater than the remaining validity period of the
security token.
When obtaining a security token with an agency, set the session_user.name parameter in the request body.
*/
CreateLoginTokenRequestBody createLoginTokenRequestBody = new CreateLoginTokenRequestBody().
      withAuth(new LoginTokenAuth().withSecuritytoken(new LoginTokenSecurityToken().
            withAccess(credential.getAccess()).
            withId(credential.getSecuritytoken()).
            withSecret(credential.getSecret()).withDurationSeconds(1800)));
CreateLoginTokenResponse createLoginTokenResponse = iamClient.createLoginToken(new
CreateLoginTokenRequest().withBody(createLoginTokenRequestBody));
String loginToken = createLoginTokenResponse.getXSubjectLoginToken();

// Login URL of the custom identity broker
String authURL = "https://auth.huaweicloud.com/authui/federation/login";
// Login URL of an enterprise management system.
String enterpriseSystemLoginURL = "https://example.com/";
// Huawei Cloud service address to access.
String targetConsoleURL = "https://console.huaweicloud.com/iam/?region=cn-north-4";

// Create a FederationProxyUrl and return it to the browser through Location.
String FederationProxyUrl = authURL + "?idp_login_url=" +
      URLEncoder.encode(enterpriseSystemLoginURL, "UTF-8") +
      "&service=" + URLEncoder.encode(targetConsoleURL, "UTF-8") +
      "&logintoken=" +URLEncoder.encode(loginToken, "UTF-8");
```

Example Code Using Python

The following Python code shows how to create a FederationProxyUrl that gives federated users direct access to the Huawei Cloud console.

```
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.http.http_config import HttpConfig
from huaweicloudsdkiam.v3 import *

import urllib


# Use the global domain name to obtain a login token.
endpoint = "https://iam.myhuaweicloud.com"

# Configure client attributes.
config = HttpConfig.get_default_config()
config.ignore_ssl_verification = True
config.proxy_protocol = "https"
config.proxy_host = "proxy.huawei.com"
config.proxy_port = 8080
credentials = GlobalCredentials(ak, sk, domain_id)
```



```
# Use the domain ID (account ID), AK, and SK of userB to initialize the specified IAM client
"{Service}Client". For details about how to create userB, see section "Creating an IAM User".
client = IamClient().new_builder(IamClient) \
    .with_http_config(config) \
    .with_credentials(credentials) \
    .with_endpoint(endpoint) \
    .build()

# CreateTemporaryAccessKeyByAgency
# Call the API used to obtain a temporary access key and security token with an agency.
# The default validity period of an access key and security token is 900 seconds, that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this example, the validity period is set to 3600 seconds, that is, 1 hour.
# When you obtain a login token with a specified validity period, ensure that the validity period of the login token is not greater than the remaining validity period of the security token.
# When obtaining a security token with an agency, set the session_user.name parameter in the request body.
assume_role_session_user = AssumeroleSessionuser(name="ExternalUser")
identity_assume_role = IdentityAssumerole(agency_name="testagency",
                                          domain_id="0525e2c87exxxxxxx",
                         session_user=assume_role_session_user,
                         duration_seconds=3600)
identity_methods = ["assume_role"]
body = CreateTemporaryAccessKeyByAgencyRequestBody(
    AgencyAuth(AgencyAuthIdentity(methods=identity_methods, assume_role=identity_assume_role)))
request = CreateTemporaryAccessKeyByAgencyRequest(body)
create_temporary_access_key_by_agency_response = client.create_temporary_access_key_by_agency(request)
credential = create_temporary_access_key_by_agency_response.credential

# CreateLoginToken
# Obtain a login token.
# The default validity period of a login token is 600 seconds, that is, 10 minutes. The value ranges from 10 minutes to 12 hours. In this example, the validity period is set to 1800 seconds, that is, half an hour.
# Ensure that the validity period of the login token is not greater than the remaining validity period of the security token.
login_token_security_token = LoginTokenSecurityToken(access=credential.access, secret=credential.secret,
                             id=credential.securitytoken, duration_seconds=1800)
body = CreateLoginTokenRequestBody(LoginTokenAuth(login_token_security_token))
request = CreateLoginTokenRequest(body)
create_login_token_response = client.create_login_token(request)
login_token = create_login_token_response.x_subject_login_token

# Obtain a custom identity broker URL.
auth_URL = "https://auth.huaweicloud.com/authui/federation/login"
# Login URL of an enterprise management system.
enterprise_system_login_URL = "https://example.com/"
# Huawei Cloud service address to access.
target_console_URL = "https://console.huaweicloud.com/iam/?region=cn-north-4"

# Create a FederationProxyUrl and return it to the browser through Location.
FederationProxyUrl = auth_URL + "?idp_login_url=" + urllib.parse.quote(
    enterprise_system_login_URL) + "&service=" + urllib.parse.quote(
    target_console_URL) + "&logintoken=" + urllib.parse.quote(login_token)
print(FederationProxyUrl)
```

10.3 Configuring a Custom Identity Broker with a Token

If the IdP of your enterprise is not compatible with SAML or OpenID Connect, you can create a custom identity broker to enable access to Huawei Cloud. You can write and run code to generate a login URL. Users in your enterprise can then use the URL to log in to Huawei Cloud. The users will be authenticated by your enterprise IdP.

> NOTE
>
> If your enterprise IdP is compatible with SAML or OpenID Connect, configure **identity federation** to enable users in your enterprise to access Huawei Cloud through SSO.

Prerequisites

- Your enterprise has an enterprise management system.
- The enterprise administrator has created an account (for example, **DomainA**) in Huawei Cloud.

Procedure

Step 1 Use the **DomainA** account to create an IAM user (for example, **UserB**) by following the instructions in **Creating an IAM User**.

Step 2 (Optional) Add **UserB** to a user group (for example, **GroupC**) and grant permissions to the user group by following the instructions in **Creating a User Group and Assigning Permissions**.

Step 3 Configure the **access key** (recommended) or username and password of **UserB** in the configuration file of your enterprise IdP so that the user can obtain a user token. For account security, encrypt the password and access keys before you store them.

Step 4 Log in to the enterprise management system, access the custom identity broker by selecting a common user from the user list. For details, see the documentation of the enterprise management system. For this example, select user **UserB** configured in step **Step 3**.

> NOTE
>
> The user list of the custom broker is the same as the IAM user list under your Huawei Cloud account. To align these IAM users with the user accounts in your enterprise, configure the IAM users' **access keys** (recommended) or usernames and passwords in the configuration file of the enterprise IdP.

Step 5 The custom identity broker uses the token of **userB** to call the API **POST / v3.0/OS-CREDENTIAL/securitytokens** used to obtain a temporary access key and security token. For details, see **Obtaining a Temporary Access Key and Security Token Through a Token**.

Step 6 The custom identity broker uses the temporary access key, security token, and global domain name of IAM (**iam.myhuaweicloud.com**) to call the API **POST / v3.0/OS-AUTH/securitytoken/logintokens** for obtaining a login token. The value of **X-Subject-LoginToken** in the response header is a login token. For details, see **Obtaining a Login Token**.

NOTE

- To obtain a login token by calling the API **POST /v3.0/OS-AUTH/securitytoken/logintokens**, use the global domain name (**iam.myhuaweicloud.com**) of IAM.
- A login token is issued to a user to log in through a custom identity broker and contains identity and session information about the user. A login token is valid for 10 minutes by default.
- You can set the validity period of a login token by calling the API **POST /v3.0/OS-AUTH/securitytoken/logintokens**. The validity period ranges from 10 minutes to 12 hours. If the value you have specified is greater than the remaining validity period of the temporary security token, the remaining validity period of the temporary security token is used.

Step 7 The custom identity broker generates a FederationProxyUrl and returns it to the browser through **Location**.

https://auth.huaweicloud.com/authui/federation/login?idp_login_url={enterprise_system_loginURL}&service={console_service_region_url}*&logintoken={logintoken}*

Example:

*https://auth.huaweicloud.com/authui/federation/login?idp_login_url=https%3A%2F%2Fexample.com&service=https%3a%2f%2fconsole.huaweicloud.com%2fapm%2f%3fregion%3dcn-north-4%23%2fapm%2fatps%2ftopology&logintoken=******

Table 10-2 Parameter description

Parameter	Description
idp_login_url	Login URL of the enterprise management system.
service	Access address of a Huawei Cloud service.
logintoken	Login token of the custom identity broker.

For details about how to create a FederationProxyUrl, view the example provided in **Creating a FederationProxyUrl Using a Token**.

NOTE

The FederationProxyUrl contains the login token that has been obtained from IAM, and the value of each parameter in the FederationProxyUrl is encoded using URLEncode.

Step 8 If the login token is authenticated successfully, federated users will be automatically redirected to the Huawei Cloud service address specified in the **service** parameter.

If the login token fails to be authenticated, federated users will be redirected to the address specified in **idp_login_url**.

----End

10.4 Creating a FederationProxyUrl Using a Token

This section provides example code used to programmatically create a FederationProxyUrl using a token for logging in to Huawei Cloud services.

Example Code Using Java

The following Java code shows how to create a FederationProxyUrl that gives federated users direct access to the Huawei Cloud console.

```
import java.net.URLEncoder;
import java.util.Collections;
import com.huaweicloud.sdk.core.auth.GlobalCredentials;
import com.huaweicloud.sdk.core.http.HttpConfig;
import com.huaweicloud.sdk.core.exception.*;
import com.huaweicloud.sdk.iam.v3.IamClient;
import com.huaweicloud.sdk.iam.v3.model.*;

// Use the global domain name to obtain a login token.
String endpoint = "https://iam.myhuaweicloud.com";

// Configure client attributes.
HttpConfig config = HttpConfig.getDefaultHttpConfig()
        .withIgnoreSSLVerification(true)
        .withProxyHost("proxy.huawei.com")
        .withProxyPort(8080);

// Use the domain ID (account ID), AK, and SK of userB to initialize the specified IAM client
"{Service}Client". For details about how to create userB, see section "Creating an IAM User".
IamClient iamClient = IamClient.newBuilder().withCredential(new GlobalCredentials()
        .withDomainId(domainId)
        .withAk(ak)
        .withSk(sk))
        .withEndpoint(endpoint)
        .withHttpConfig(config)
        .build();

/*CreateTemporaryAccessKeyByToken
Call the API used to obtain a temporary access key and security token with a token.
The default validity period of an access key and security token is 900 seconds, that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this example, the validity period is set to 3600 seconds, that is, 1 hour.
When you obtain a login token with a specified validity period, ensure that the validity period of the login token is not greater than the remaining validity period of the security token.
*/
TokenAuthIdentity tokenAuthIdentity = new
TokenAuthIdentity().withMethods(Collections.singletonList(TokenAuthIdentity.MethodsEnum.fromValue("token"))).withToken(new IdentityToken().withDurationSeconds(3600));
CreateTemporaryAccessKeyByTokenRequestBody createTemporaryAccessKeyByTokenRequestBody = new
CreateTemporaryAccessKeyByTokenRequestBody().withAuth(new
TokenAuth().withIdentity(tokenAuthIdentity));
CreateTemporaryAccessKeyByTokenResponse createTemporaryAccessKeyByTokenResponse =
iamClient.createTemporaryAccessKeyByToken(new
CreateTemporaryAccessKeyByTokenRequest().withBody(createTemporaryAccessKeyByTokenRequestBody));
Credential credential = createTemporaryAccessKeyByTokenResponse.getCredential();

/*CreateLoginToken
Obtain a login token.
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 default validity period of a login token is 600 seconds, that is, 10 minutes. The value ranges from 10 minutes to 12 hours. In this example, the validity period is set to 1800 seconds, that is, half an hour.
Ensure that the validity period of the login token is not greater than the remaining validity period of the security token.
*/
CreateLoginTokenRequestBody createLoginTokenRequestBody = new CreateLoginTokenRequestBody().
        withAuth(new LoginTokenAuth().withSecuritytoken(new LoginTokenSecurityToken().
                withAccess(credential.getAccess()).
                withId(credential.getSecuritytoken()).
                withSecret(credential.getSecret()).withDurationSeconds(1800)));
CreateLoginTokenResponse createLoginTokenResponse = iamClient.createLoginToken(new
CreateLoginTokenRequest().withBody(createLoginTokenRequestBody));
```



```
String loginToken = createLoginTokenResponse.getXSubjectLoginToken();

// Obtain a custom identity broker URL.
String authURL = "https://auth.huaweicloud.com/authui/federation/login";
// Login URL of an enterprise management system.
String enterpriseSystemLoginURL = "https://example.com/";
// Huawei Cloud service address to access.
String targetConsoleURL = "https://console.huaweicloud.com/iam/?region=cn-north-4";

// Create a FederationProxyUrl and return it to the browser through Location.
String FederationProxyUrl = authURL + "?idp_login_url=" +
        URLEncoder.encode(enterpriseSystemLoginURL, "UTF-8") +
        "&service=" + URLEncoder.encode(targetConsoleURL, "UTF-8") +
        "&logintoken=" +URLEncoder.encode(loginToken, "UTF-8");
```

Example Code Using Python

The following Python code shows how to create a FederationProxyUrl that gives federated users direct access to the Huawei Cloud console.

```
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.http.http_config import HttpConfig
from huaweicloudsdkiam.v3 import *

import urllib

# Use the global domain name to obtain a login token.
endpoint = "https://iam.myhuaweicloud.com"

# Configure client attributes.
config = HttpConfig.get_default_config()
config.ignore_ssl_verification = True
config.proxy_protocol = "https"
config.proxy_host = "proxy.huawei.com"
config.proxy_port = 8080
credentials = GlobalCredentials(ak, sk, domain_id)

# Use the domain ID (account ID), AK, and SK of userB to initialize the specified IAM client
"{Service}Client". For details about how to create userB, see section "Creating an IAM User".
client = IamClient().new_builder(IamClient) \
    .with_http_config(config) \
    .with_credentials(credentials) \
    .with_endpoint(endpoint) \
    .build()

# CreateTemporaryAccessKeyByToken
# Call the API used to obtain a temporary access key and security token with a token.
# The default validity period of an access key and security token is 900 seconds, that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this example, the validity period is set to 3600 seconds, that is, 1 hour.
# When you obtain a login token with a specified validity period, ensure that the validity period of the login token is not greater than the remaining validity period of the security token.
identity_methods = ["token"]
identity_token = IdentityToken(duration_seconds=3600)
body = CreateTemporaryAccessKeyByTokenRequestBody(
    TokenAuth(TokenAuthIdentity(methods=identity_methods, token=identity_token)))
request = CreateTemporaryAccessKeyByTokenRequest(body)
create_temporary_access_key_by_token_response = client.create_temporary_access_key_by_token(request)
credential = create_temporary_access_key_by_token_response.credential

# CreateLoginToken
# Obtain a login token.
# 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 default validity period of a login token is 600 seconds, that is, 10 minutes. The value ranges from 10 minutes to 12 hours. In this example, the validity period is set to 1800 seconds, that is, half an hour.
# Ensure that the validity period of the login token is not greater than the remaining validity period of the
```



```
security token.
login_token_security_token = LoginTokenSecurityToken(access=credential.access, secret=credential.secret,
                             id=credential.securitytoken, duration_seconds=1800)
body = CreateLoginTokenRequestBody(LoginTokenAuth(login_token_security_token))
request = CreateLoginTokenRequest(body)
create_login_token_response = client.create_login_token(request)
login_token = create_login_token_response.x_subject_login_token


# Login URL of the custom identity broker
auth_URL = "https://auth.huaweicloud.com/authui/federation/login"
# Login URL of an enterprise management system.
enterprise_system_login_URL = "https://example.com/"
# Huawei Cloud service address to access.
target_console_URL = "https://console.huaweicloud.com/iam/?region=cn-north-4"

# Create a FederationProxyUrl and return it to the browser through Location.
FederationProxyUrl = auth_URL + "?idp_login_url=" + urllib.parse.quote(
    enterprise_system_login_URL) + "&service=" + urllib.parse.quote(
    target_console_URL) + "&logintoken=" + urllib.parse.quote(login_token)
print(FederationProxyUrl)
```


11 MFA Authentication

11.1 Overview

What Is MFA Authentication?

MFA authentication provides an additional layer of protection on top of the username and password. If MFA authentication is enabled, you need to enter the username and password (first factor) as well as a verification code (second factor) when performing certain operations. These factors together keep your account and resources secure.

MFA authentication can also be enabled to verify a user's identity before the user is allowed to perform critical operations.

MFA Authentication Methods

MFA authentication can be performed through SMS, email, virtual MFA device, and security key.

- Virtual MFA: A virtual MFA device generates 6-digit verification codes based on the Time-based One-time Password Algorithm (TOTP). Software-based virtual MFA devices (authenticator apps) can run on mobile devices (such as smartphones) and are easy to use. After a virtual MFA device is added, users need to enter dynamic verification codes generated from MFA devices in addition to their credentials during login.
- Security key: A security key uses a password plus a hardware device for two-factor authentication to protect resources and privacy. Currently, Huawei Cloud supports security keys based on the fast identity online (FIDO) protocol and Windows Hello. After a FIDO-based hardware MFA device, such as Yubikey, is added, users need to insert the device and touch it to verify their identities in addition to entering their credentials during login. After a Windows Hello security key is added, users need to pass identity verification with their fingerprint, PIN, or facial information.

Application Scenarios

MFA authentication is suitable for login protection and critical operation protection. You can bind a virtual MFA device to an IAM user for login protection

and operation protection. Security keys are used for login protection only. If MFA authentication is enabled, the setting takes effect for both the management console and REST APIs.

- Login protection: When you or an IAM user logs in to the console, you and the user need to enter a verification code in addition to the username and password.
- Operation protection: When you or an IAM under your account attempts to perform a critical operation, such as deleting an ECS resource, you and the user need to enter a verification code to proceed.

For more information about login protection and critical operation protection, see **Critical Operation Protection**.

Constraints

- An IAM user can have to only one virtual MFA device added.
- An IAM user can have a maximum of eight security keys added.

11.2 Configuring a Virtual MFA Device

This section describes how to **bind** and **unbind** a virtual MFA device. If the bound virtual MFA device of an IAM user is deleted or the mobile phone on which it runs is unavailable, you can **remove** the virtual MFA device for the IAM user.

This section describes how to **add** and **unbind** a virtual MFA device.

Binding a Virtual MFA Device

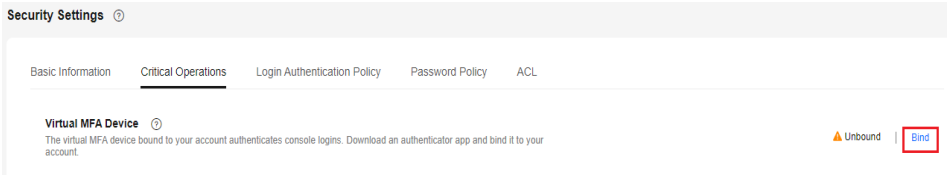
Before binding a virtual MFA device, install an authenticator app (such as Google Authenticator or Microsoft Authenticator) on your mobile device first.

- **Huawei Cloud Account**

Step 1 Go to the **Security Settings** page.

Step 2 Click the **Critical Operations** tab, and click **Bind** in the **Virtual MFA Device** row.

Figure 11-1 Virtual MFA device



Step 3 Set up the MFA application by scanning the QR code or manually entering the secret key.

You can bind a virtual MFA device to your account by scanning the QR code or entering the secret key.

- Scanning the QR code

Open the MFA application on your mobile phone, and use the application to scan the QR code displayed on the **Bind Virtual MFA Device** page. Your account or IAM user is then added to the application.

- Manually entering the secret key

  Open the MFA application on your mobile phone, and enter the secret key.

  NOTE

  The user can be manually added only using time-based one-time passwords (TOTP). You are advised to enable automatic time setting on your mobile device.

Step 4 View the verification codes on the MFA application. The code is automatically updated every 30 seconds.

Step 5 On the **Bind Virtual MFA Device** page, enter two consecutive verification codes and click **OK**.

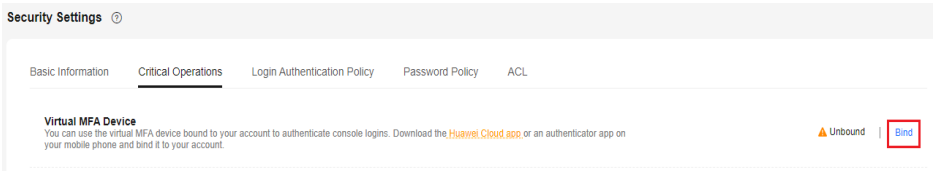
----End

- **HUAWEI ID**

Step 1 Go to the **Security Settings** page.

Step 2 Click the **Critical Operations** tab, and click **Bind** in the **Virtual MFA Device** row.

Figure 11-2 Binding a virtual MFA device



Step 3 On the **Account & security** page of the HUAWEI ID account center, associate an authenticator with your HUAWEI ID as instructed.

----End

- **IAM User**

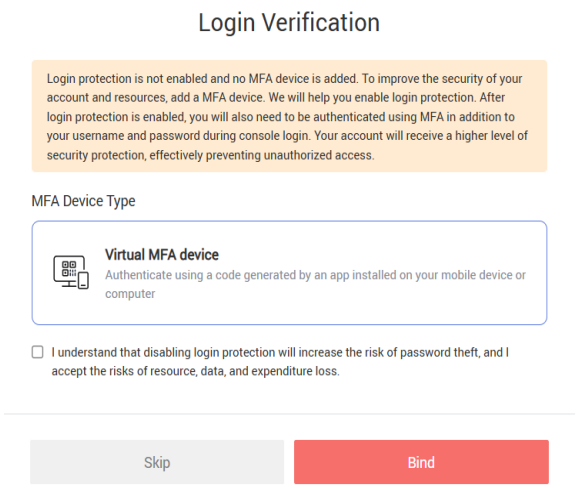
IAM users can bind a virtual MFA device on the IAM console. The procedure is the same as that for **binding a virtual MFA device for a Huawei Cloud account**.

If login protection is enabled for an IAM user and a virtual MFA device is used for authentication, or the user has bound a mobile number or email address but has not bound any virtual MFA device, the user needs to bind or rebind a virtual MFA device during login. The procedure is as follows:

Step 1 Log in to the management console as an IAM user.

Step 2 In the **Login Verification** dialog box, click **Bind**.

Figure 11-3 Login verification



Step 3 On the slide-out panel, follow the prompts to bind a virtual MFA device.

----End

Obtaining an MFA Verification Code

If virtual MFA–based login protection or operation protection is enabled, you need to enter an MFA verification code when you log in to the console or performing a critical operation.

Open the MFA application on your smart device, view the verification code displayed next to your account, and then enter the code on the console.

Unbinding a Virtual MFA Device

You can unbind the virtual MFA device as long as the mobile phone bound to the virtual MFA device is available and the virtual MFA device is still installed on your phone.

- IAM user: If the mobile phone of an IAM user is unavailable or the virtual MFA device has been deleted from the phone, request the administrator to **remove the virtual MFA device**.
- Account: If the mobile phone associated with the account is unavailable or the virtual MFA device has been deleted from the phone, contact customer service to remove the virtual MFA device.

Step 1 Go to the **Security Settings** page.

Step 2 Click the **Critical Operations** tab, and click **Unbind** in the **Virtual MFA Device** row.

NOTE

If you have upgraded your Huawei Cloud account to a HUAWEI ID, you will be redirected to the HUAWEI ID website. Go to the **Account center** > **Account and security** page, and click **Disassociate** in the **Authenticator** row in the **Security verification** area.

Step 3 On the **Unbind Virtual MFA Device** page, enter a verification code generated by the MFA application.

Figure 11-4 Entering a virtual MFA verification code

Step 4 Click **OK**.

----End

Removing the Virtual MFA Device

Account: If the mobile phone associated with the is unavailable or the virtual MFA device has been deleted from the phone, contact customer service to remove the virtual MFA device.

IAM user: If the mobile phone of an IAM user is unavailable or the virtual MFA device has been deleted from the user's phone, contact the **administrator** to remove the virtual MFA device. The administrator needs to perform the following steps:

Step 1 Log in to the IAM console.

Step 2 On the **Users** page, click **Security Settings** in the row containing the user for whom you want to remove the bound virtual MFA device.

Step 3 On the **Security Settings** tab page, click **Remove** in the **Virtual MFA Device** row.

Step 4 Click **OK**.

----End

11.3 Configuring a Security Key

This section describes how to add and unbind a security key. For details, see **Adding a Security Key** and **Unbinding a Security Key**.

Constraints

- Security keys added to IAM users can only be used for login protection.
- An IAM user can have a maximum of eight security keys added.

Adding a Security Key

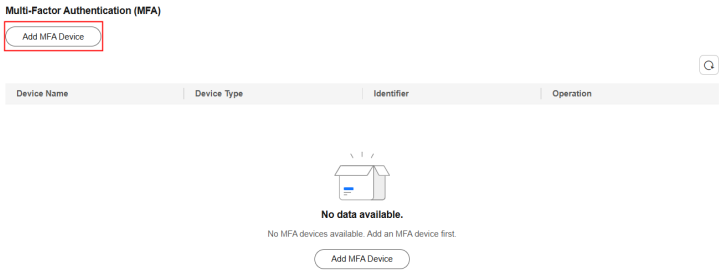
Step 1 Log in to the **IAM console** as the administrator.

Step 2 In the user list, click a username or click **Security Settings** in the **Operation** column to access the user details page.

Step 3 Click the **Security Settings** tab and locate the **Multi-Factor Authentication (MFA)** area.

Step 4 Click **Add MFA Device**.

Figure 11-5 Adding an MFA device



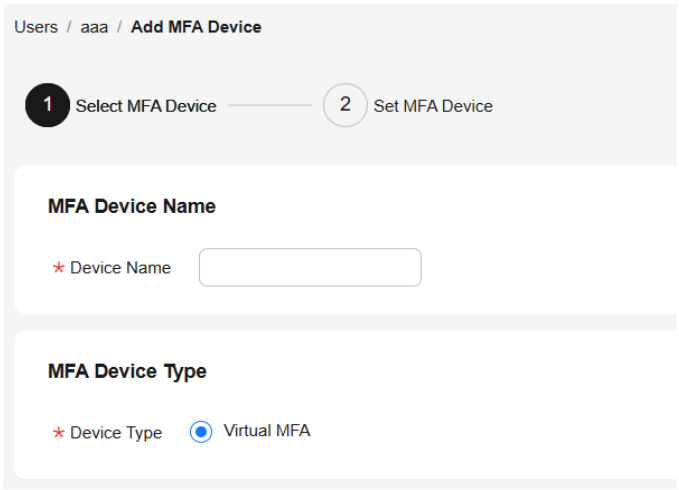
Step 5 In the slide-out panel on the right, set the MFA device name.

Only letters, digits, hyphens (-), and underscores (_) are allowed.

Step 6 Select **Security key** for **Device Type** and click **Next**.

Step 7 To set up Windows Hello, select an authentication method in the displayed dialog box.

Figure 11-6 Setting up Windows Hello



NOTE

If the device does not support facial recognition, the facial recognition option will not be displayed.

Step 8 To set up a FIDO security key, click **Cancel** in the displayed dialog box.

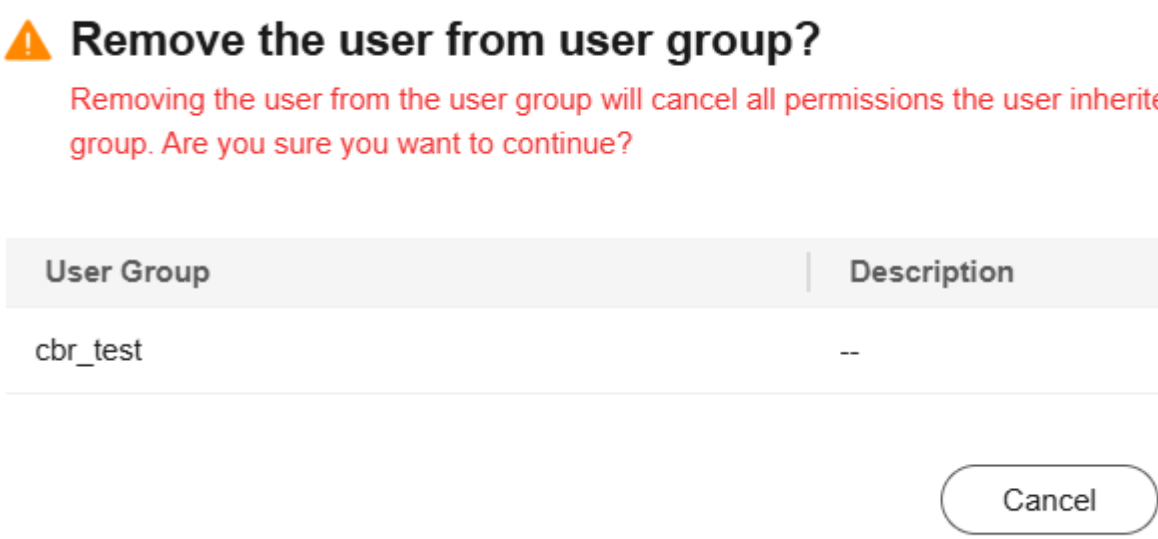
Step 9 In the new dialog box, click **OK**.

Step 10 Insert the security key into the USB port of the computer and tap the button on the key.

Step 11 In the displayed dialog box, click **OK**.

Step 12 After the verification is successful, a dialog box is displayed, indicating that the MFA device is added. Click **OK**. The MFA device will be displayed in the MFA device list.

Figure 11-7 MFA device added



----End

Unbinding a Security Key

Step 1 Log in to the **IAM console** as the administrator.

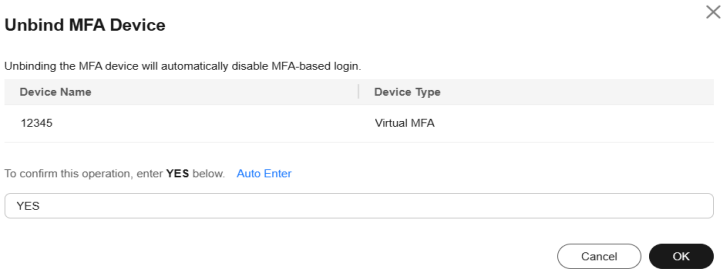
Step 2 In the user list, click a username or click **Security Settings** in the **Operation** column to access the user details page.

Step 3 Click the **Security Settings** tab.

Step 4 Click **Unbind** in the **Operation** column of the target security key.

Step 5 In the displayed dialog box, enter **YES** in the text box.

Figure 11-8 Confirming unbinding



Step 6 Click **OK**.

----End

12 CTS Auditing

12.1 Key IAM Operations Supported by CTS

Scenarios

CTS records operations performed on cloud resources in your account. The operation logs can be used to perform security analysis, track resource changes, perform compliance audits, and locate faults.

It is recommended that you enable the CTS service to record key IAM operations, such as creating and deleting users.

Procedure

Step 1 Log in to the management console.

Step 2 If you log in to Huawei Cloud using an account, go to **Step 3**. If you log in as an IAM user, request the administrator to grant you the following permissions:

- Security Administrator
- CTS FullAccess

For details, see **Assigning Permissions to an IAM User**.

Step 3 Choose **Service List** > **Management & Governance** > **Cloud Trace Service**.

Step 4 On the displayed authorization page, click **Enable and Authorize**.

NOTE

- When using CTS, you must have the required permissions for relevant operations, but do not need to be granted the **Security Administrator** role again.
- After you enable CTS, the system automatically creates two trackers to record management traces, that is, operations (such as creation, login, and deletion) performed on all cloud resources.
  - In the **current region**, a tracker is created to record management traces of all project-level services deployed in this region.
  - In the **CN-Hong Kong** region, a tracker is created to record management traces of all global services, such as IAM.

----End

CTS records all operations performed on IAM, such as creating users and user groups. **Table 12-1** shows the IAM operations that can be recorded by CTS.

Table 12-1 IAM operations that can be recorded by CTS

Operation	Resource Type	Trace Name
User login	user	login
User login failed (Account login failures not included)	user	loginFailed
User logout	user	logout
Login using a QR code	user	scanQRCodeLogin
Login using a QR code failed	user	scanQRCodeLoginFailed
Login via OpenID succeeded	user	oidcLoginSuccess
Login via OpenID Connect failed	user	oidcLoginFailed
Login via SSO succeeded	user	iamUserSsoLoginSuccess
Login via SSO failed	user	iamUserSsoLoginFailed
Resetting the password	user	fpwdResetSuccess
Creating an IAM user	user	createUser

Operation	Resource Type	Trace Name
Changing the email address or mobile number	user	updateUser
Deleting a user	user	deleteUser
Changing the password	user	updateUserPwd
Setting a password for a user (by the administrator)	user	updateUserPwd
Modifying login protection of an IAM user	user	modifyLoginProtect
Changing the mobile number using an email	user	changeMobileByEmail
Changing the password using an email	user	updateUserPwdByEmail
Initial federated login succeeded	user	tenantLoginBySamlSuccess
Federated login using a custom identity broker succeeded	user	federationLoginNoPwdSuccess
Federated login using a custom identity broker failed	user	federationLoginNoPwdFailed
Creating a user group	userGroup	createGroup
Modifying a user group	userGroup	updateGroup
Deleting a user group	userGroup	deleteGroup
Adding users to a user group	userGroup	addUserToGroup
Removing users from a user group	userGroup	removeUserFromGroup

Operation	Resource Type	Trace Name
Unbinding a virtual MFA device	MFA	UnBindMFA
Binding a virtual MFA device	MFA	BindMFA
Creating a security key	mfa	createWebauthnMfaDevice
Enabling security key	mfa	enableWebauthnMfaDevice
Creating a project	project	createProject
Modifying a project	project	updateProject
Deleting a project	project	deleteProject
Creating an agency	agency	createAgency
Modifying an agency	agency	updateAgency
Deleting an agency	agency	deleteAgency
Switching an agency	agency	switchRole
Assigning all project permissions to an agency	agency	updateAgencyInheritedGrants
Revoking all project permissions from an agency	agency	deleteAgencyInheritedGrants
Assigning global service permissions to an agency	agency	updateAgencyAssignsByRole
Assigning global service permissions to an agency (API)	roleAgencyDomain	assignRoleToAgencyOnDomain

Operation	Resource Type	Trace Name
Updating agency permissions	agency	updateAgencyAssignsByRole
Registering an identity provider	identityProvider	createIdentityProvider
Modifying an identity provider	identityProvider	updateIdentityProvider
Deleting an identity provider	identityProvider	deleteIdentityProvider
Updating an identity conversion rule	identityProvider	updateMapping
Updating the identity provider metadata	identityProvider	metadataConfiguration
Manually editing metadata of a preset IdP	identityProvider	metadataConfiguration
Registering a mapping	mapping	createMapping
Updating a mapping	mapping	updateMapping
Deleting a mapping	mapping	deleteMapping
Registering a protocol	identityProvider	createProtocol
Updating a protocol	identityProvider	updateProtocol
Deleting a protocol	identityProvider	deleteProtocol
Revoking global service permissions from an agency	roleAgencyDomain	unassignRoleToAgencyOnDomain

Operation	Resource Type	Trace Name
Assigning project permissions to an agency	roleAgencyProject	assignRoleToAgencyOnProject
Revoking project permissions from an agency	roleAgencyProject	unassignRoleToAgencyOnProject
Modifying the login authentication policy	SecurityPolicy	modifySecurityPolicy
Modifying the password policy	SecurityPolicy	modifySecurityPolicy
Modifying the ACL	SecurityPolicy	modifySecurityPolicy
Modifying the login authentication policy	loginpolicy	securitypolicy
Modifying the password policy	passwordpolicy	securitypolicy
Modifying the ACL	acl	securitypolicy
Creating an account	domain	createDomain
Update an account	domain	updateDomain
Delete an account	domain	deleteDomain
Logging failed via OpenID Connect	domain	oidcLoginFailed
Creating a custom policy	Policy	createRole
Modifying a custom policy	Policy	updateRole
Deleting a custom policy	Policy	deleteRole

Operation	Resource Type	Trace Name
Assigning global service permissions to a user group (API)	assignment	createAssignment
Assigning global service permissions to a user group	group	updateGroupAssignsByRole
Revoking global service permissions from a user group	assignment	deleteAssignment
Creating a permanent AK/SK	credential	createCredential
Updating a permanent access key (AK/SK)	credential	updateCredential
Deleting a permanent access key (AK/SK)	credential	deleteCredential
Disabling or enabling an access key (AK/SK)	credential	updateCredential
Creating temporary access keys on the console as a federated user	credential	CreateTemporaryAccessKeyFromConsole
Assigning permissions to users or enterprise projects	assignment	grantRoleToUserOnEnterpriseProject
Revoking permissions from users or enterprise projects	enterpriseProject	revokeRoleFromUserOnEnterpriseProject

Operation	Resource Type	Trace Name
Updating user group permissions for enterprise projects	enterpriseProject	updateRoleFromGroupOnEnterprisePro-ject
Creating a user group	group	createGroup
Deleting a user group	group	deleteGroup

12.2 Viewing CTS Traces in the Trace List

Scenarios

After you enable Cloud Trace Service (CTS) and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, CTS starts recording operations on data in Object Storage Service (OBS) buckets. CTS stores operation records (traces) generated in the last seven days.

This section describes how to query or export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces 5 minutes later.
- These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

Viewing Real-Time Traces in the Trace List of the New Edition

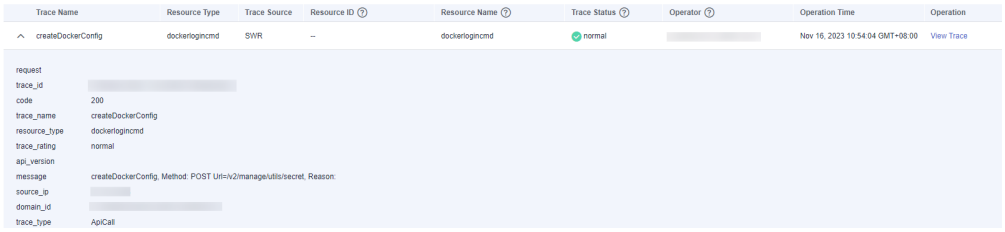
1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.

3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.
   - **Operator**: Select one or more operators from the drop-down list.
   - **Trace Status**: Select **normal**, **warning**, or **incident**.
     - **normal**: The operation succeeded.
     - **warning**: The operation failed.
     - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
   - **Enterprise Project ID**: Enter an enterprise project ID.
   - **Access Key**: Enter a temporary or permanent access key ID.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
   - Enter any keyword in the search box and press **Enter** to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
   - Click to view the latest information about traces.
   - Click to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled ( ), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

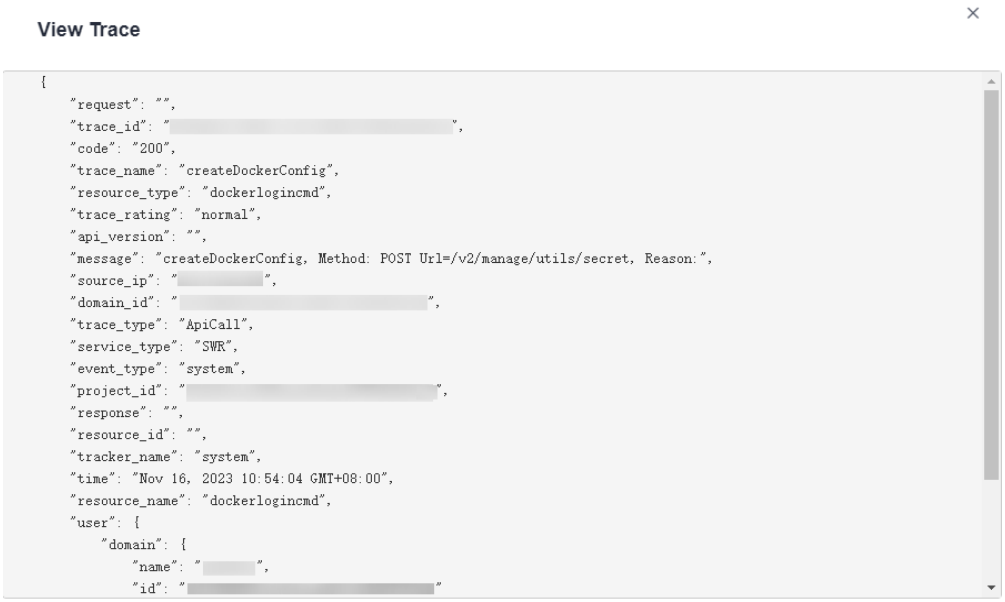
Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.

2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available.
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
   - Click ↻ to view the latest information about traces.
8. Click ⌄ on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

13 Quota Adjustment

What Is a Quota?

A quota is a limit on the quantity or capacity of a certain type of service resources that a user can use, for example, the maximum number of IAM users or user groups that you can create.

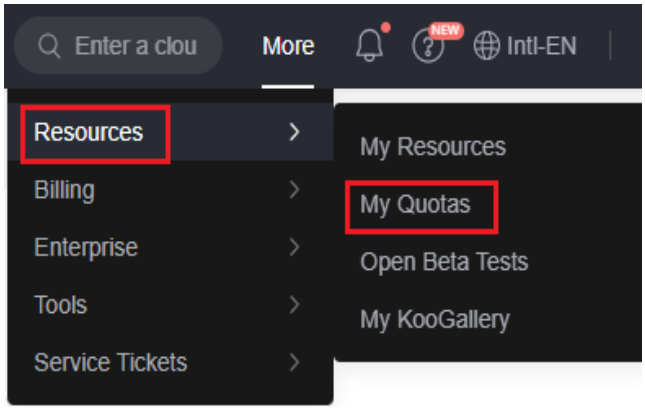
If the current resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Quotas** page is displayed.

   Figure 13-1 My quotas

3. On the **Quotas** page, view the used and total quotas of each type of resources.

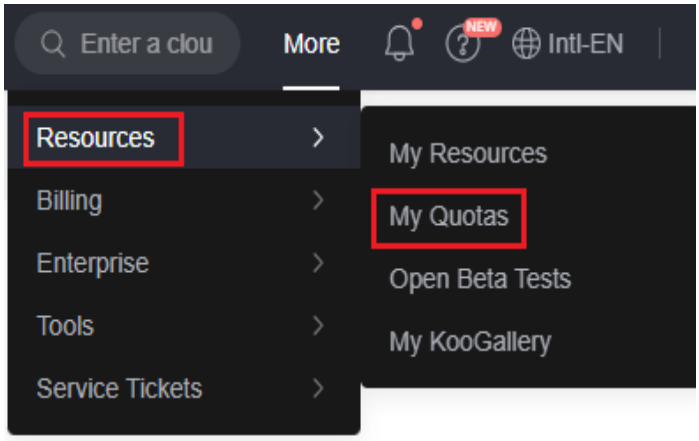
   If the quota cannot meet your service requirements, increase the quota.

How Do I Increase My Quota?

1. Log in to the management console.

2. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Quotas** page is displayed.

   Figure 13-2 My Quotas



3. Click **Increase Quota**.
4. On the **Create Service Ticket** page, set the parameters.
   In the **Problem Description** area, enter the required quota and the reason for the quota adjustment.
5. Read the agreements and confirm that you agree to them, and then click **Submit**.

