IAM Identity Center

User Guide

Issue 01

Date 2025-05-16

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 User Management

1.1 Creating Users

After IAM Identity Center is enabled, you need to create users. You can associate an IAM Identity Center user with multiple accounts in your organization and configure permissions for the user. Then, you can log in to the system as the IAM Identity Center user to access resources of those accounts without repeated login.

If you are using IAM Identity Center for the first time, the service enabling page is displayed. Click **Enable Now** to enable IAM Identity Center first.

Procedure

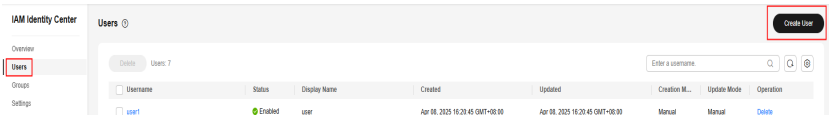
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Users**.

Step 4 Click **Create User** in the upper right corner of the page.

Figure 1-1 Creating users



Step 5 Configure basic information about the user. After the configuration is complete, click **Next** in the lower right corner of the page.

The user details are mandatory. The contact methods, job-related information, and address are optional and can be set as needed.

Figure 1-2 Configuring basic information

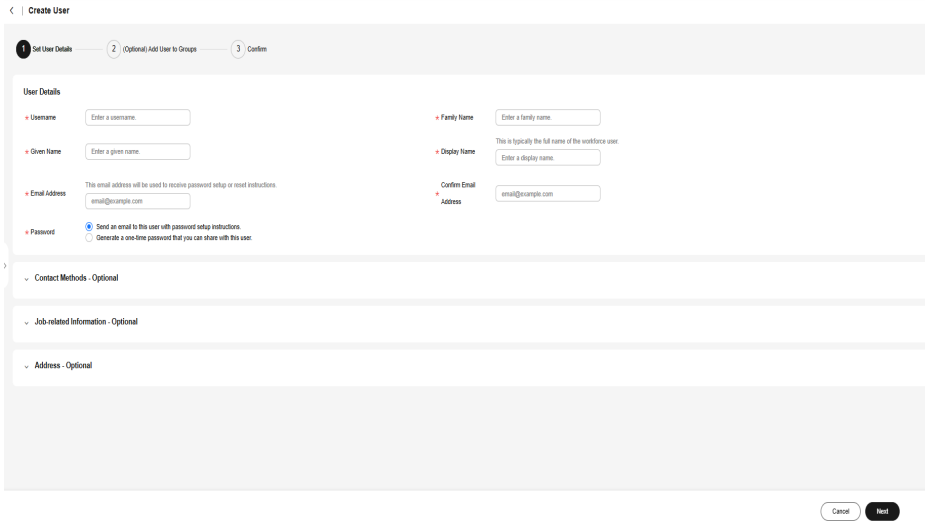


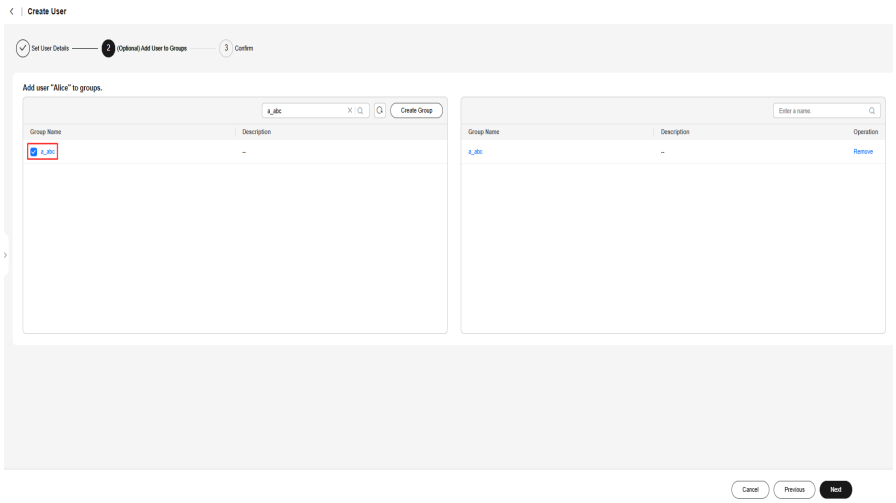
Table 1-1 User details

Parameter	Description
Username	IAM Identity Center username. The value is user-defined and must be unique.
Password	Select a password generation method. • **Send an email to this user with password setup instructions**: The system will send a password reset instruction email to the user. The user can set a password as instructed. • **Generate a one-time password that you can share with this user**: An automatically generated one-time password will be displayed on the page indicating that the user is created. The administrator copies the information and sends it to the user. When the user uses the one-time password to log in through the user portal URL, the system prompts the user to change the password. The user can only log in to the console using the new password. **CAUTION** If the page is closed, the one-time password generated by the system will no longer be displayed again. To obtain the password again, you need to **reset the password**.
Email Address	Email address of a user. The value is user-defined and must be unique. It can be used to authenticate the user and reset the password.
Confirm Email Address	Enter the email address again for confirmation. The email address and confirm email address must be the same.
Family Name	Family name of the user.

Parameter	Description
Given Name	Given name of the user.
Display Name	Display name of an IAM Identity Center user. The value is user-defined and can be the same as the display name of another IAM Identity Center user. Generally, the value is the real name of the user.

Step 6 (Optional) In the **(Optional) Add User to Groups** step, select groups. The user will have the permissions assigned to the group. Click **Next**.

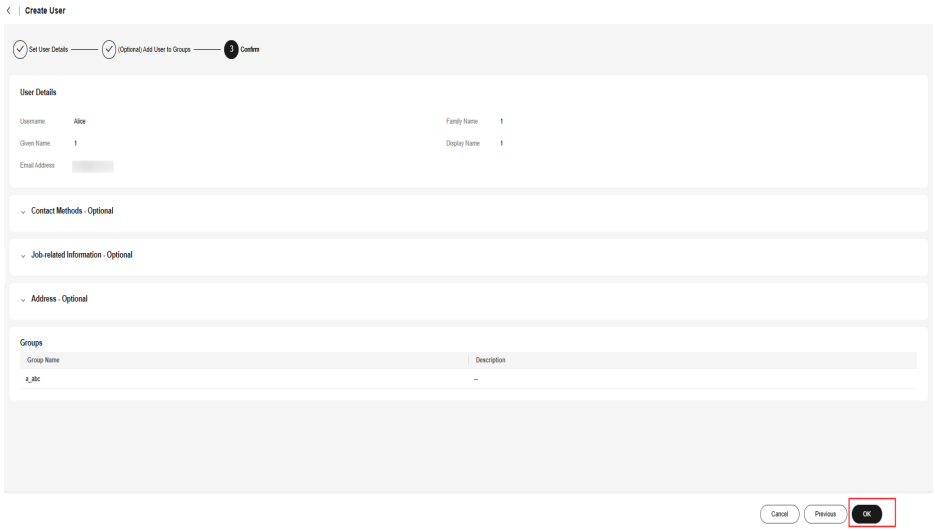
Figure 1-3 (Optional) Adding a user to groups



Step 7 In the **Confirm** step, confirm the configuration and click **OK** in the lower right corner of the page. The IAM Identity Center user is created and displayed in the user list.

- If **Send an email to this user with password setup instructions.** is selected for **Password** in step **Step 5**, the user list will be displayed, showing the newly created IAM Identity Center user.
- If **Generate a one-time password that you can share with this user.** is selected for **Password** in step **Step 5**, a page that contains detailed information about the one-time password will be displayed. You can copy the information and send it to the user. The user can use the username and one-time password to log in through the user portal URL.

Figure 1-4 Confirming user creation



----End

1.2 Logging In as an IAM Identity Center User and Accessing Resources

You can use an IAM Identity Center username and password to log in to the management console through the user portal URL. You need to associate the user with permission sets and one or more member accounts in your organization so that the user can access resources under those accounts according to the permissions assigned to the permission sets. For details, see **Creating a Permission Set** and **Associating Accounts with Users/Groups and Permission Sets**.

IAM Identity Center provides a single user portal URL for all of your IAM Identity Center users to log in to the management console. The administrator can change the user portal URL once. For details, see **Customizing User Portal URL**.

Procedure

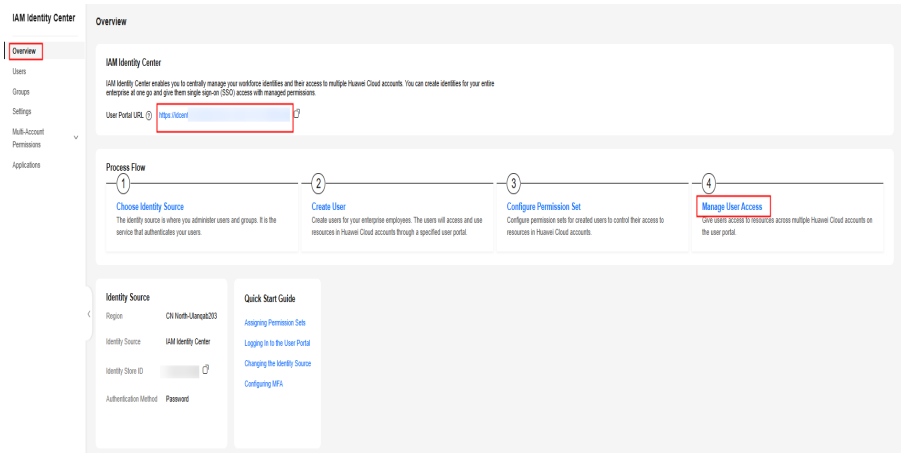
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Dashboard**. On the displayed page, obtain the user portal URL.

The user portal URL can also be obtained from the password setting instruction email sent to the user or from the one-time password page displayed when the user was created.

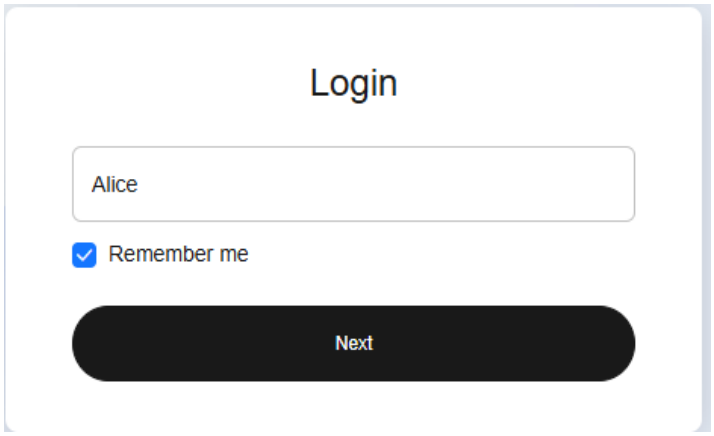
Figure 1-5 User portal URL



Step 4 Open a browser and access the user portal URL. Enter the IAM Identity Center username, and click **Next**.

The IAM Identity Center username and password for logging in to the portal are obtained during user creation. For details, see **Creating Users**. If the password is forgotten or needs to be changed, the administrator can use the **password resetting** function to allow the system to resend a password setting instruction email to the user or generate a one-time password.

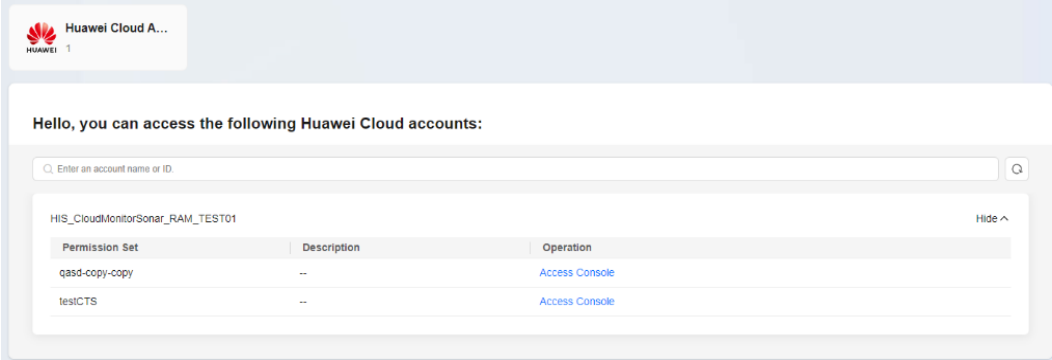
Figure 1-6 User login



Step 5 Enter the password, and click **Log In**.

Step 6 Under a specific account, locate your desired permission set and click **Access Console** in the **Operation** column to access resources according to the permissions included in the permission set.

Figure 1-7 Accessing resources



----End

1.3 Managing Users

After an IAM Identity Center user is created, you can view and modify user details, reset the password, disable, enable, or delete the user, and add the user to or remove the user from a group.

This section includes the following content:

- **Modifying User Details**
- **Disabling, Enabling, or Deleting a User**
- **Resetting a Password**
- **Adding a User to or Removing a User from Groups**

Modifying User Details

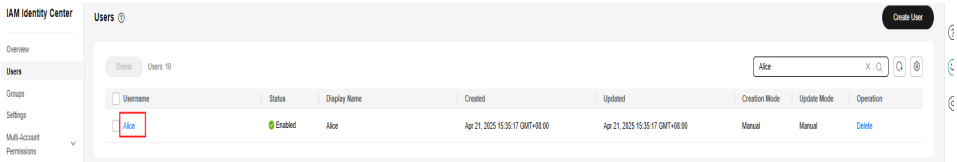
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Users**.

Step 4 In the user list, click a username to go to the user details page.

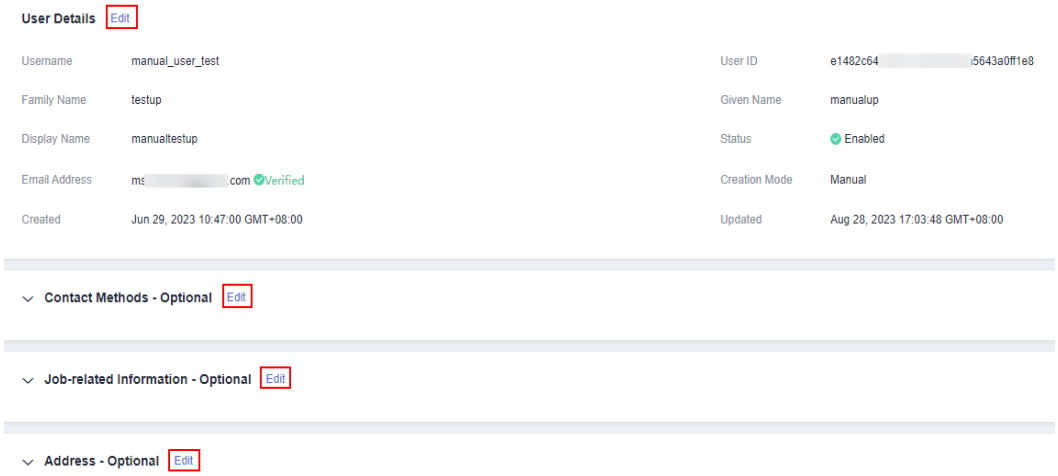
Figure 1-8 Selecting a user



Step 5 Click **Edit** in the **User Details** area to modify the user details.

Step 6 (Optional) Click **Edit** in the **Contact Methods**, **Job-related Information**, and **Address** to modify related information.

Figure 1-9 Modifying user information



Step 7 After the editing is complete, click **Save**.

----End

Disabling, Enabling, or Deleting a User

You can disable the access permissions of an IAM Identity Center user that is not required temporarily. You can enable it again if needed.

You can also delete IAM Identity Center users. Deleted users cannot be restored. Exercise caution when performing this operation.

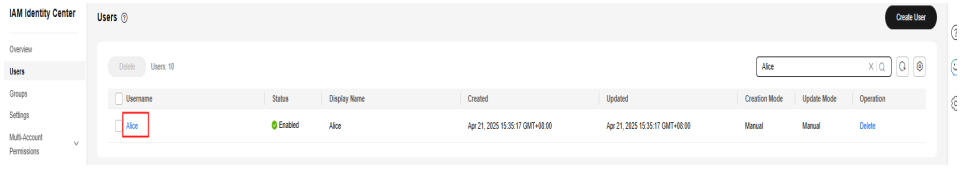
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Users**.

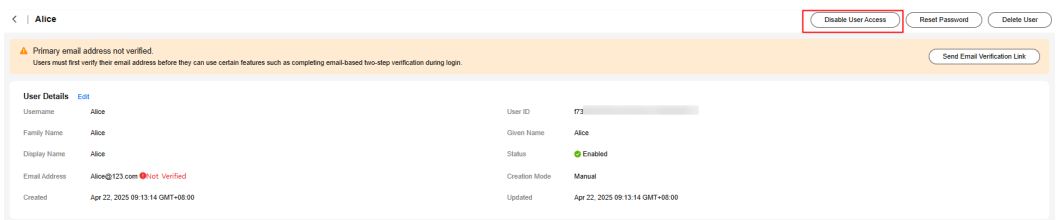
Step 4 In the user list, click a username to go to the user details page.

Figure 1-10 Selecting a user



Step 5 In the upper right corner on the displayed page, click **Disable**.

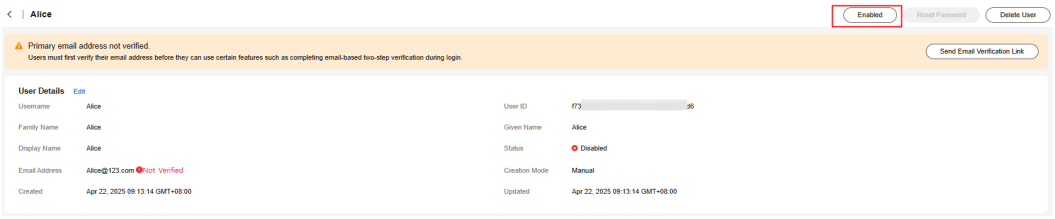
Figure 1-11 Disabling a user



Step 6 In the displayed dialog box, click **OK**. Check that the status of the IAM Identity Center user changes to **Disabled**.

Step 7 To enable a user, click the name of the disabled user in the user list. On the displayed user details page, click **Enable** in the upper right corner.

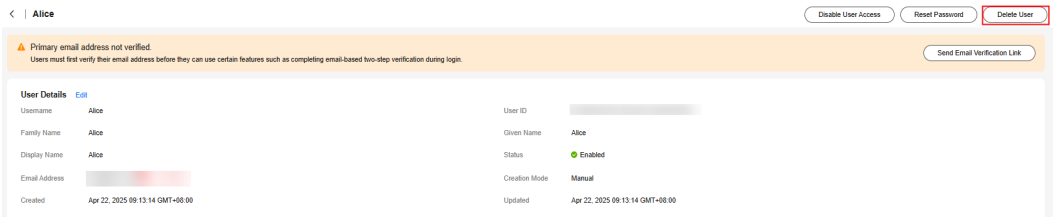
Figure 1-12 Enabling a user



Step 8 In the displayed dialog box, click **OK**. Check that the status of the IAM Identity Center user changes to **Enabled**.

Step 9 To delete a user, on the user details page, click **Delete User** in the upper right corner.

Figure 1-13 Deleting a user



Step 10 Click **OK** in the displayed dialog box.

----End

Resetting a Password

You can use the password resetting function to change the password of an IAM Identity Center user.

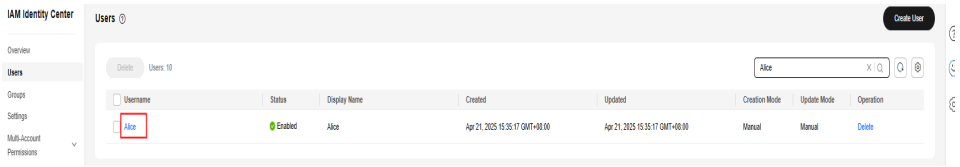
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Users**.

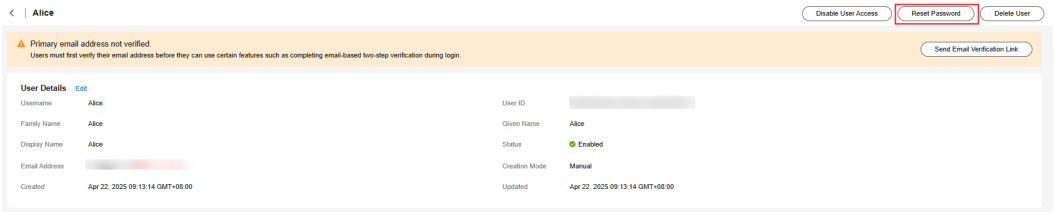
Step 4 In the user list, click a username to go to the user details page.

Figure 1-14 Selecting a user



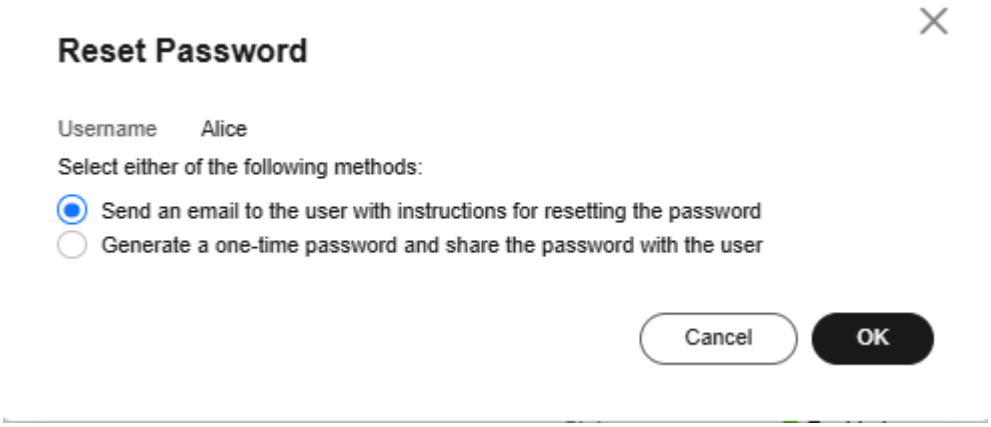
Step 5 Click **Reset Password** in the upper right corner of the page.

Figure 1-15 Resetting a password



Step 6 In the displayed dialog box, select a password resetting method and click **OK**.

Figure 1-16 Selecting a password resetting method



Password resetting methods:

- **Send an email to this user with password setup instructions**: The system will send a password reset instruction email to the user. The user can reset the password as instructed.
- **Generate a one-time password that you can share with this user**: The system will display the detailed information about the one-time password. The administrator can copy the information and send it to the user. The user can use the username and one-time password to log in through the user portal URL.

----End

Adding a User to or Removing a User from Groups

After an IAM Identity Center user is created, you can add it to or remove it from groups.

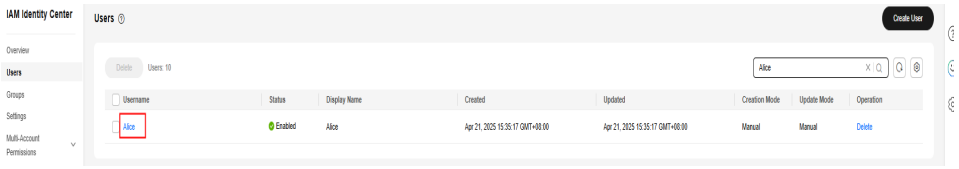
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Users**.

Step 4 In the user list, click a username to go to the user details page.

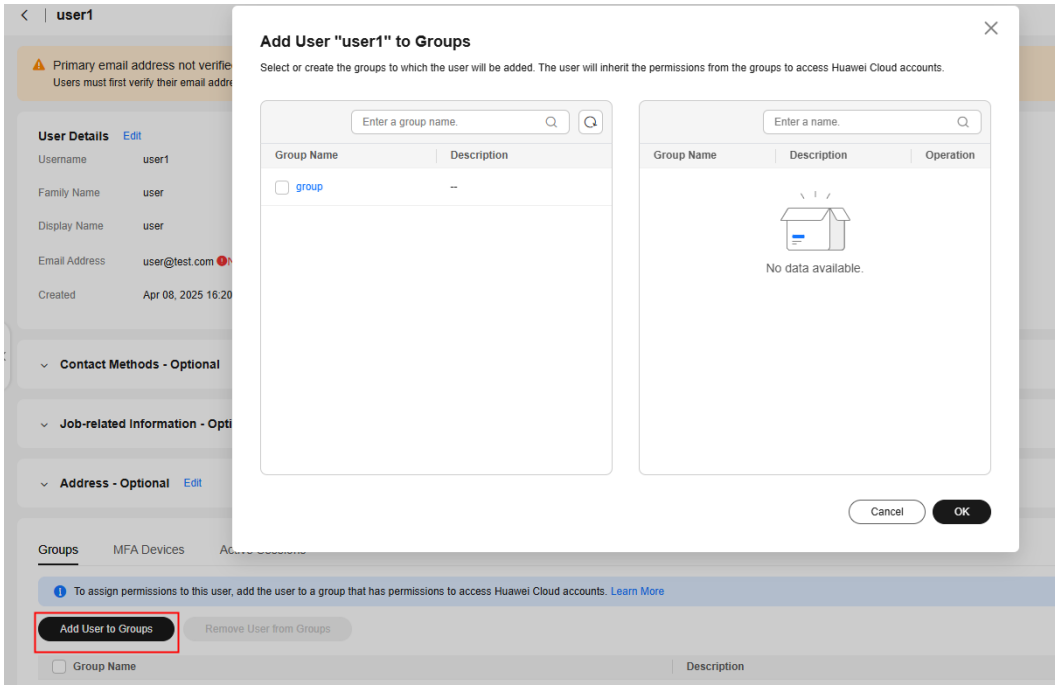
Figure 1-17 Selecting a user



Step 5 On the **Groups** tab in the lower part of the user details page, click **Add User to Groups**.

Step 6 In the displayed group list, select the groups to which the user is to be added and click **OK**.

Figure 1-18 Adding a user to groups

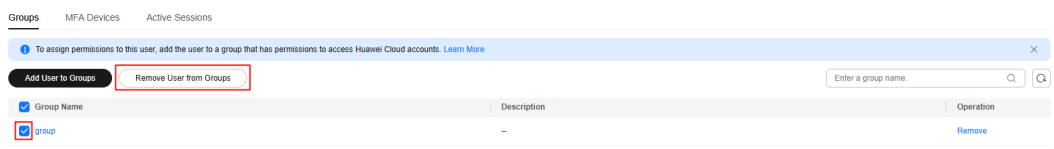


Step 7 In the group list, select the groups from which the user is to be removed and click **Remove User from Groups**.

Alternatively, click **Remove** in the **Operation** column of a specific group.

Step 8 Click **OK** in the displayed dialog box.

Figure 1-19 Removing a user from groups



----End

1.4 Deleting a User

You can delete an IAM Identity Center user that is no longer needed. Deleting an IAM Identity Center user deletes all information about the user and revokes its access permissions.

Deleted users cannot be restored. Exercise caution when performing this operation.

Deleting a User

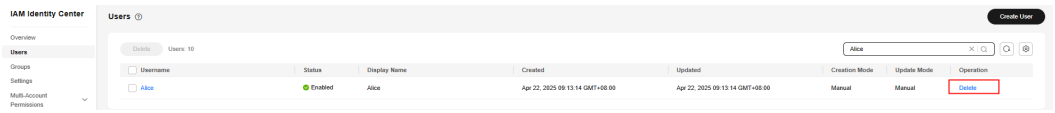
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Users**.

Step 4 In the user list, locate the user to be deleted and click **Delete** in the **Operation** column.

Figure 1-20 Deleting a user



Step 5 Click **OK** in the displayed dialog box.

----End

Batch Deleting Users

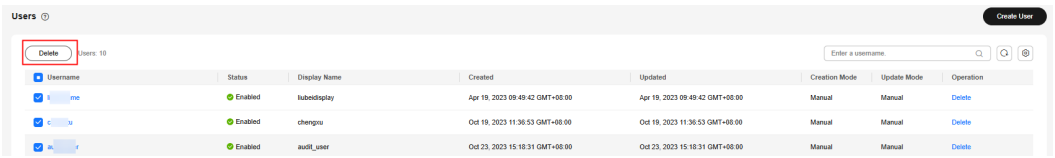
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Users**.

Step 4 In the user list, select multiple users and click **Delete** above the list.

Figure 1-21 Batch deleting users



Step 5 Click **OK** in the displayed dialog box.

----End

1.5 Configuring the Duration of the User Portal Session

By default, the session duration of the user portal is 8 hours, which means the maximum duration for a user to log in to the user portal without re-authentication is 8 hours. After the maximum session duration expires, the user logs out of the user portal and needs to be authenticated again. You can set the duration as follows:

NOTE

If you use an external identity provider (IdP) as the identity source of IAM Identity Center, the duration of the user portal session is the shorter one that you set in the IdP or IAM Identity Center. For example, if your IdP session duration is 24 hours and you set the session duration to 18 hours in IAM Identity Center, your users must be authenticated again in the user portal after 18 hours.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

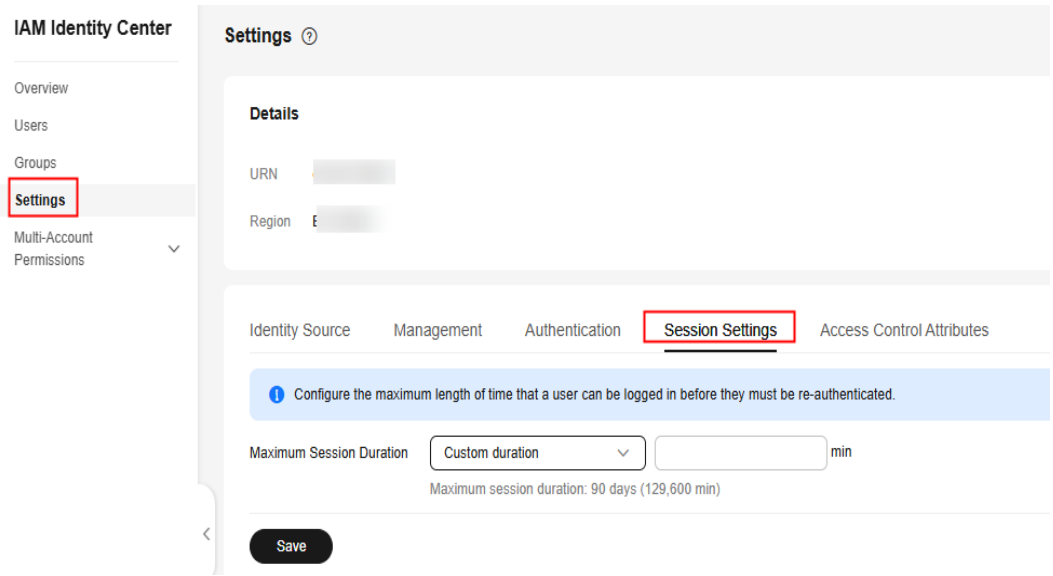
Step 3 Choose **Settings** in the navigation pane.

Step 4 On the **Session Settings** tab, configure the maximum duration of a session for accessing the user portal.

The maximum session duration is 8 hours by default. You can change the duration from 15 minutes to 90 days.

The drop-down list provides common durations for you to select.

Figure 1-22 Session settings



Step 5 Click **Save**.

----End

2 Group Management

2.1 Creating a Group

Administrators can create IAM Identity Center groups, associate permission sets and accounts with the groups, and add IAM Identity Center users to these groups so that these users inherit permissions from the groups.

Procedure

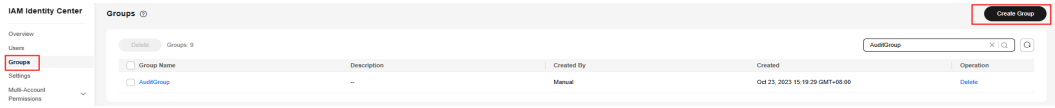
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Groups**.

Step 4 Click **Create Group** in the upper right corner of the page.

Figure 2-1 Creating a group



Step 5 On the displayed page, enter a group name and description.

The group name must be unique in IAM Identity Center.

Step 6 (Optional) Select users to be added to this group.

Step 7 Click **OK**. An IAM Identity Center group is created and displayed in the group list.

----End

2.2 Adding Users to or Removing Users from a Group

After an IAM Identity Center user is added to or removed from a specific IAM Identity Center group, the user gains or loses the permissions of that group. This way, you can change the user's permissions quickly.

If a user is added to multiple groups, the user inherits the permissions from all these groups.

Adding Users to a Group

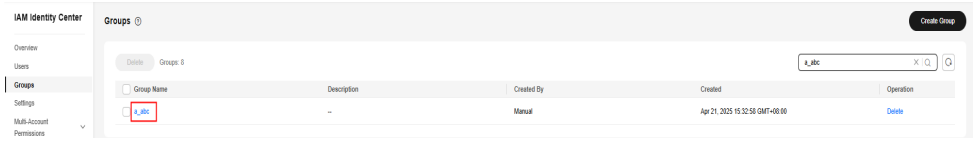
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Groups**.

Step 4 In the group list, click a group name.

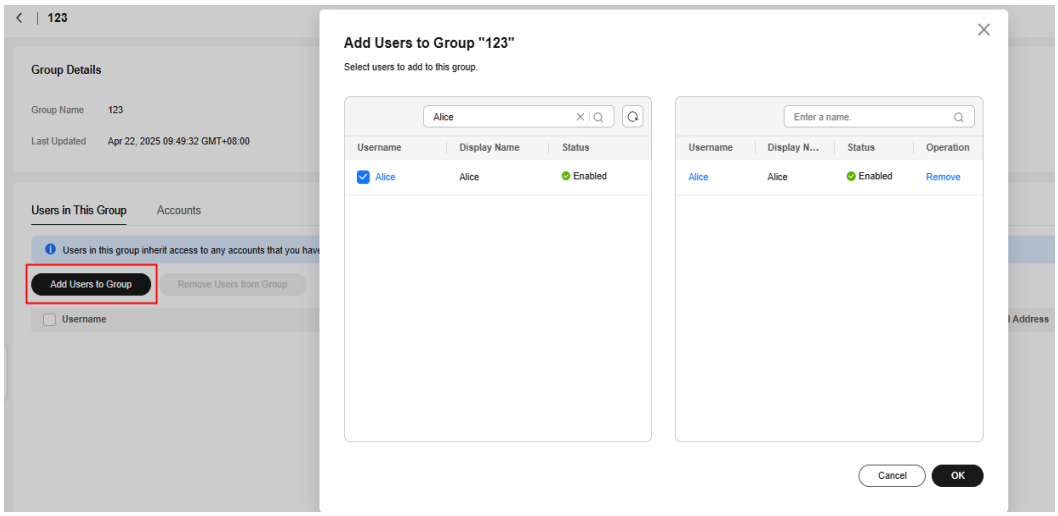
Figure 2-2 Selecting a group



Step 5 In the **Users in This Group** area, click **Add User to Group**.

Step 6 In the user list, select the user to be added to the group and click **OK**.

Figure 2-3 Adding users to a group



----End

Removing Users from a Group

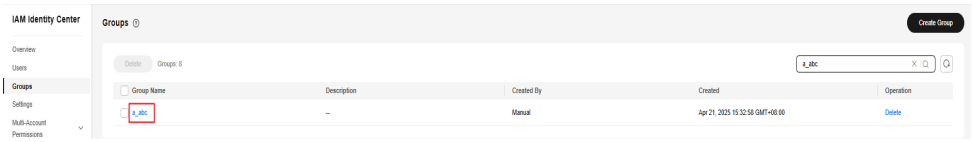
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Groups**.

Step 4 In the group list, click a group name.

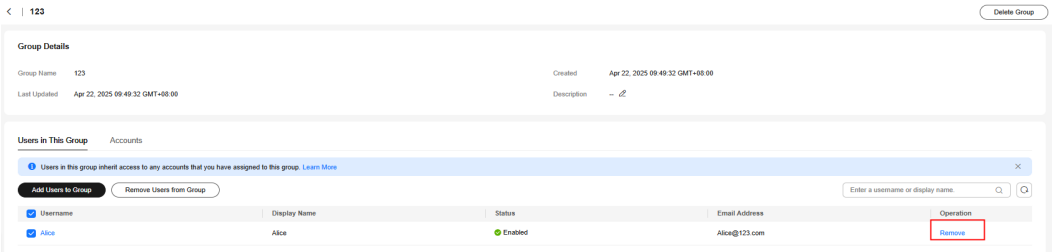
Figure 2-4 Selecting a group



Step 5 In the user list, locate the user to be removed and click **Remove** in the **Operation** column.

Step 6 Click **OK** in the displayed dialog box.

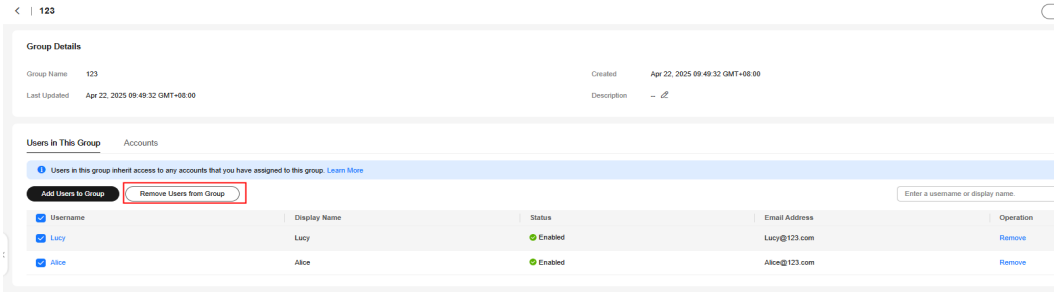
Figure 2-5 Removing a user from a group



Step 7 In the user list, select multiple users to be removed and click **Remove User from Group**.

Step 8 Click **OK** in the displayed dialog box.

Figure 2-6 Batch removing users



----End

2.3 Deleting a Group

You can delete an IAM Identity Center group that is no longer needed. After a group is deleted, all users in the group will lose the permissions attached to the group.

Deleted groups cannot be restored. Exercise caution when performing this operation.

Deleting a Group

Step 1 Log in to the Huawei Cloud management console.

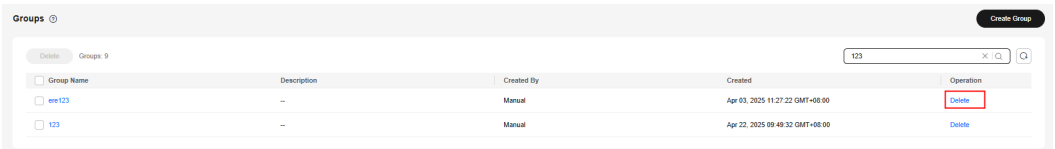
Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Groups**.

Step 4 In the group list, locate the row that contains the group to be deleted and click **Delete** in the **Operation** column.

Step 5 Click **OK** in the displayed dialog box.

Figure 2-7 Deleting a group



----End

Batch Deleting Groups

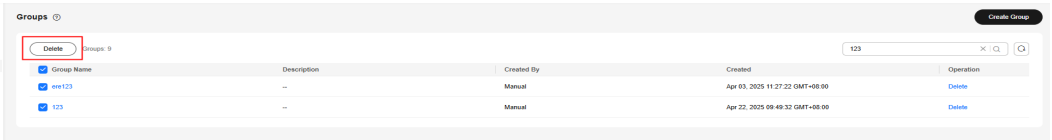
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Groups**.

Step 4 In the group list, select multiple groups and click **Delete** above the list.

Figure 2-8 Batch deleting groups



Step 5 Click **OK** in the displayed dialog box.

----End

2.4 Viewing the Accounts Associated With a User Group

You can view the accounts associated with a user group and the permission sets assigned to the account.

Procedure

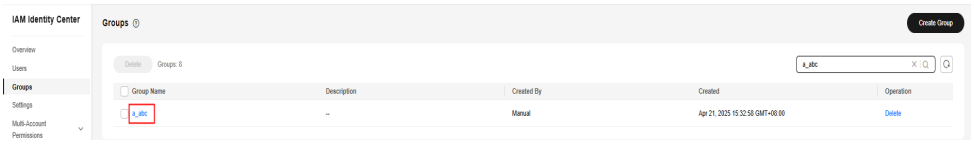
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Groups**.

Step 4 In the group list, click a group name.

Figure 2-9 Selecting a group



Step 5 On the user group details page, click the **Accounts** tab. You can view which accounts are associated with the user group and the permission sets assigned to the account.

Figure 2-10 Viewing account associations

----End

3 Multi-Account Permissions Management

3.1 Registering a Delegated Administrator

By default, only the Organizations management account can use and manage IAM Identity Center. The management account can delegate administration of IAM Identity Center to a member account in your organization to extend the ability to manage IAM Identity Center.

This operation will delegate IAM Identity Center administrative access permissions to users in this member account. All users who have sufficient permissions for the delegated administrator account can perform all IAM Identity Center administrative tasks from this account, except for:

- Deleting IAM Identity Center
- Registering other member accounts as delegated administrators
- Managing assignments to the management account
- Enabling or disabling access permissions of a user
- Managing permission sets provisioned to the management account

Prerequisites

Before registering a delegated administrator, you need to enable IAM Identity Center as a trusted service in the Organizations service.

Procedure

Step 1 Log in to the Huawei Cloud management console.

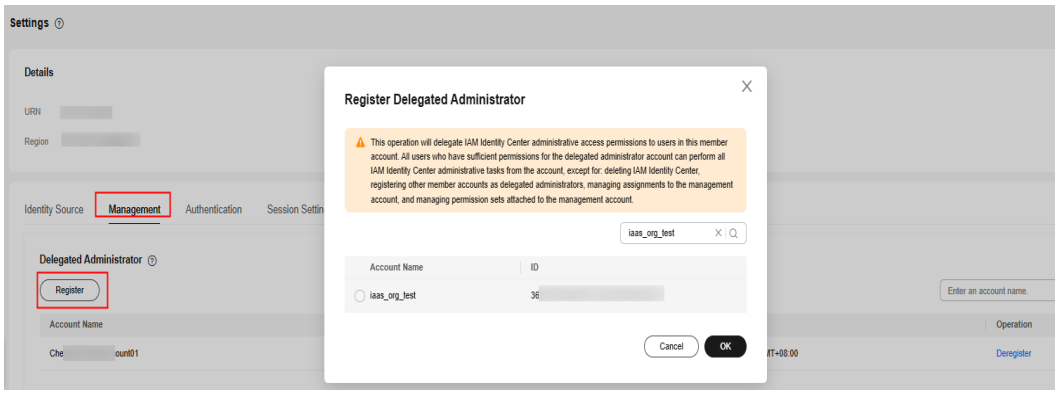
Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 On the **Management** tab, click **Register**.

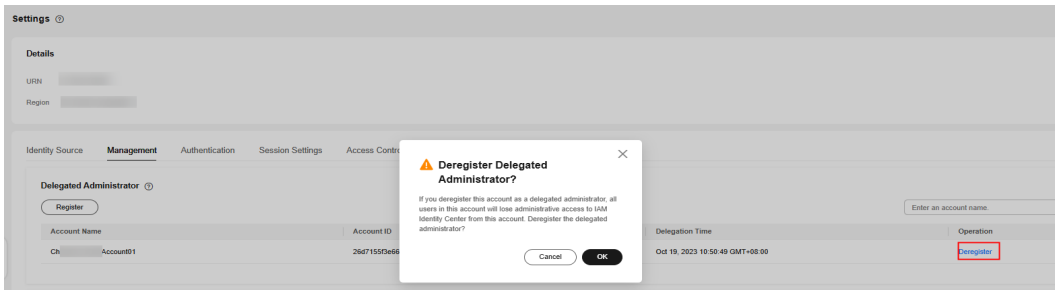
Step 5 In the displayed dialog box, select a member account and click **OK**.

Figure 3-1 Registering a delegated administrator



Step 6 In the delegated administrator list, locate the target account and click **Deregister** in the **Operation** column. After the deregistration, this account will lose administrative access to IAM Identity Center.

Figure 3-2 Deregistering a delegated administrator



----End

3.2 Permission Sets

3.2.1 Creating a Permission Set

A permission set is a template created and maintained by an administrator. It defines one or more IAM policies. Permission sets simplify the assignment of account access for users and groups in IAM Identity Center. With permission sets, you do not need to configure permissions for accounts individually.

Creating permission sets is mandatory. When logging in to the management console as an IAM Identity Center user to access resources of multiple accounts, you must associate the user with permission sets. Otherwise, the user cannot access any resources after login.

IAM provides system-defined policies to define common actions supported by cloud services. When creating a permission set, you can directly choose from these IAM system-defined policies. System-defined policies cannot be modified. You can create a custom identity policy or custom policy in IAM Identity Center to supplement system-defined policies. For details about system-defined policies for all cloud services, see **System-defined Permissions**.

NOTE

A permission set can include a maximum of 18 system-defined policies, one custom identity policy, and one custom policy.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Multi-Account Permissions** > **Permission Sets**.

Step 4 Click **Create Permission Set** in the upper right corner of the page.

Figure 3-3 Creating a permission set

Step 5 In the **Set Permission Set Details** step, configure details about the permission set and click **Next**.

Figure 3-4 Setting permission set details

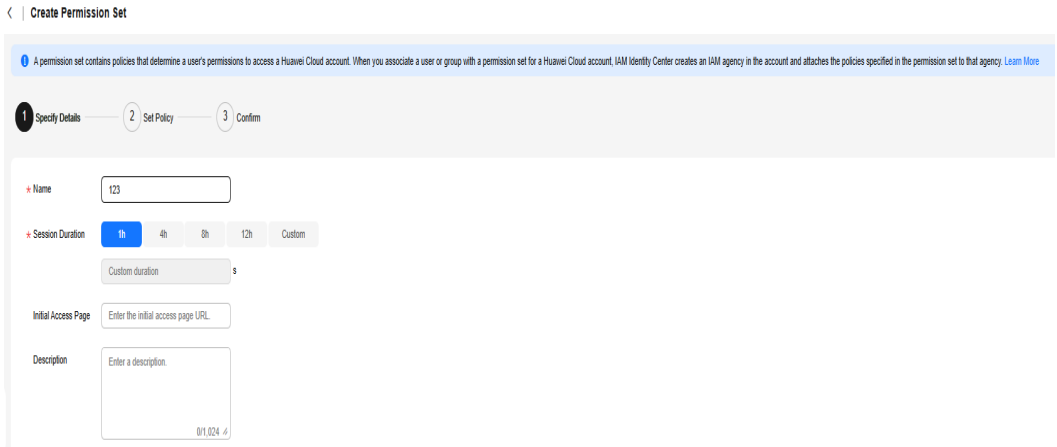


Table 3-1 Permission set details

Parameter	Description
Name	Name of a permission set. The value is user-defined and must be unique.
Session Duration	The length of time a user can be logged in to the console. When the login time exceeds the configured session duration, the user is automatically logged out. To continue the access, the user needs to log in again.

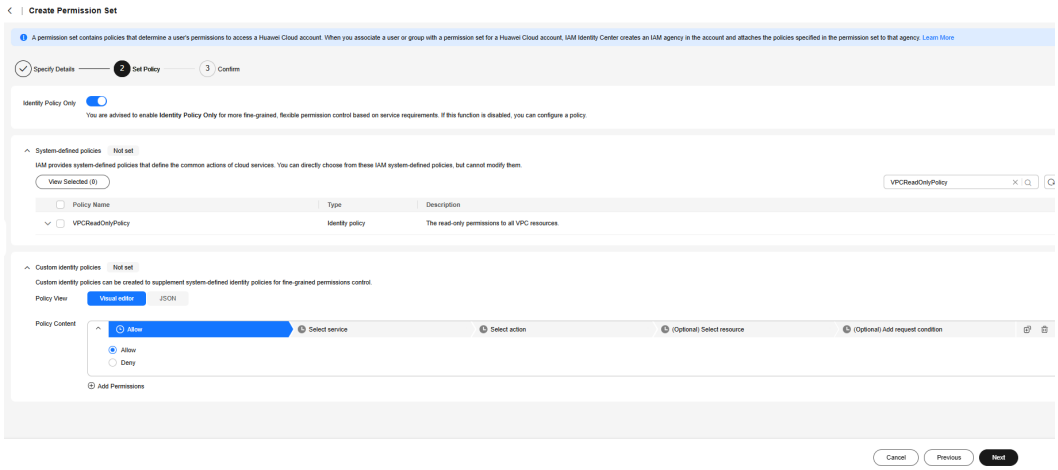
Parameter	Description
Initial Access Page	Initial page that a user accesses after logging in to the console using the user portal URL. For example, if you enter the IAM console URL, users will access the IAM console after login.
Description	Description of a permission set.

Step 6 In the **Set Policy** step, configure system-defined policies, custom identity policies, and custom policies for the permission set and click **Next**.

If you enable **Identity Policy**, only system-defined policies and custom identity policies are displayed.

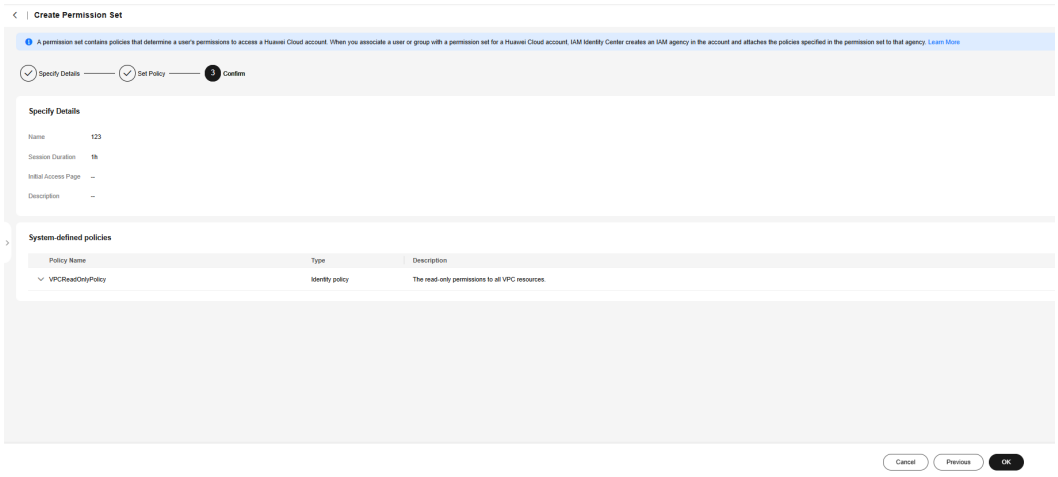
- System-defined policies: You can select system-defined policies preconfigured in IAM Identity Center, including policies and identity policies.
- Custom identity policies: You can create custom identity policies in visual editor or JSON view to supplement system-defined identity policies.
- Custom policies: You can create custom policies only in JSON view to supplement system-defined policies.

Figure 3-5 Setting policies



Step 7 In the **Confirm** step, confirm the configuration and click **OK** in the lower right corner.

Figure 3-6 Confirming configurations



NOTE

By default, newly created permission sets are not attached to any accounts. Their status will change to **Attached** after you attach them to accounts.

----End

3.2.2 Viewing or Modifying a Permission Set

After a permission set is created, you can view or modify the permission set details and policy settings that the permission set uses, and update the permission set for associated accounts.

Viewing Permission Set Details

Step 1 Log in to the Huawei Cloud management console.

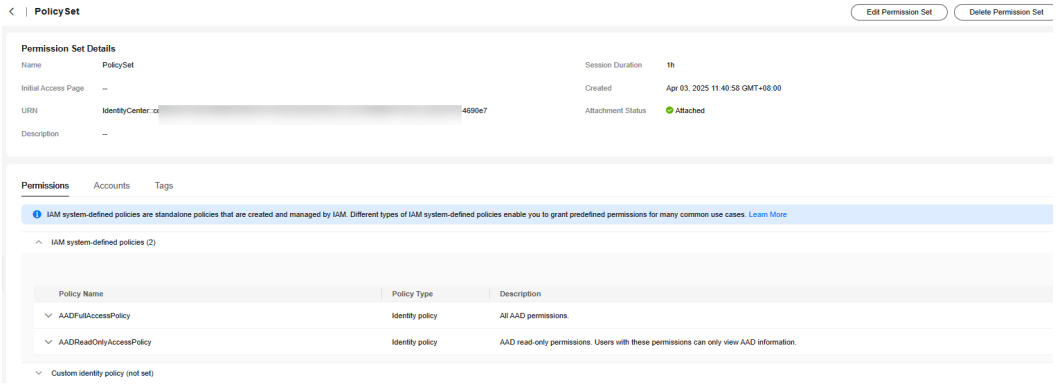
Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Multi-Account Permissions** > **Permission Sets**.

Step 4 View the created permission sets and their details in the list.

Step 5 In the permission set list, click the name of a permission set to view its details, including permissions, accounts, and tags.

Figure 3-7 Permission set details



----End

Editing a Permission Set

Step 1 Log in to the Huawei Cloud management console.

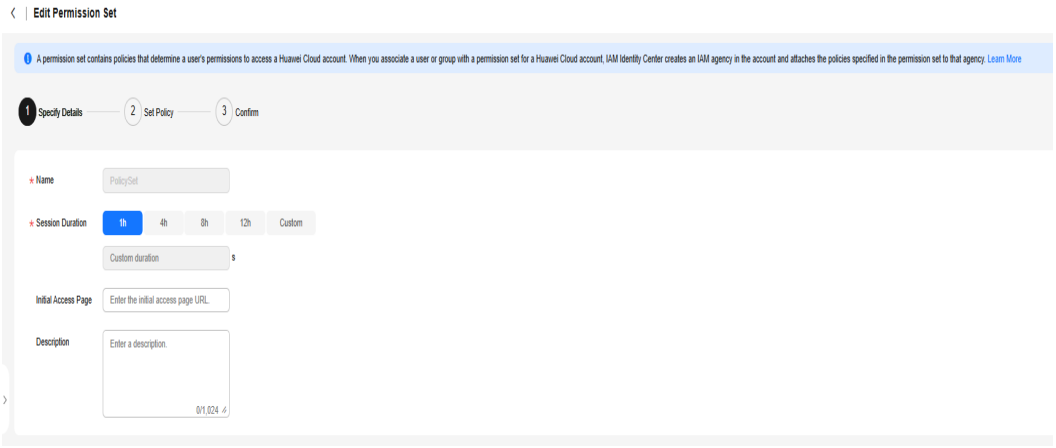
Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Multi-Account Permissions** > **Permission Sets**.

Step 4 In the permission set list, click **Edit** in the **Operation** column of the target permission set.

Step 5 In the **Specify Details** step on the displayed page, modify the session duration, initial access page, and description of the permission set, and then click **Next**.

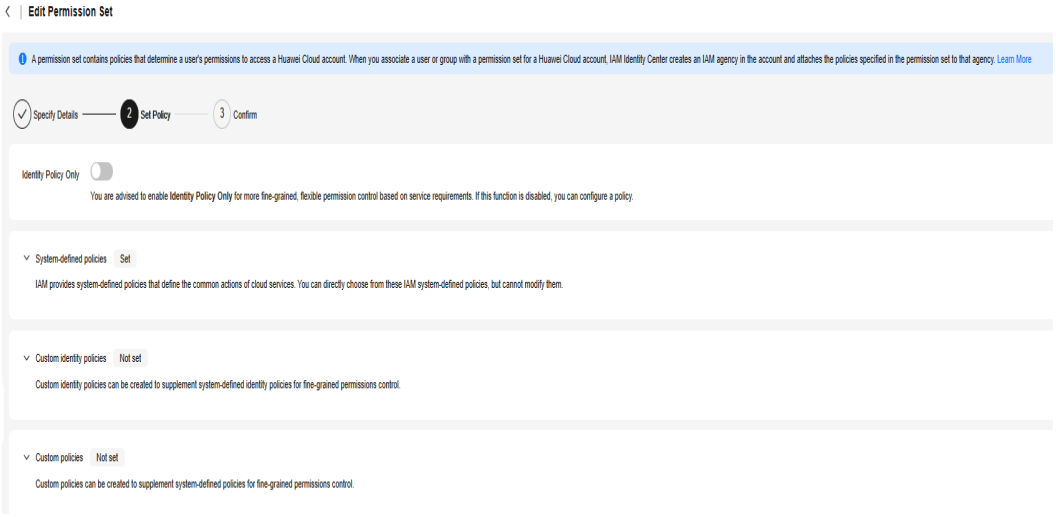
Figure 3-8 Specifying details



Step 6 In the **Set Policy** step, modify system-defined policies, custom identity policies, and custom policies and click **Next**. You can also choose whether to enable **Identity Policy**.

If policies and custom policies have been configured in the permission set, enabling identity policy will delete them.

Figure 3-9 Setting policies



Step 7 In the **Confirm** step, confirm the modification and click **OK**.

----End

Updating a Permission Set

If a permission set fails to be updated, the permission set status in the account list changes to **Outdated**. To update the permission set, do as follows:

Step 1 Log in to the Huawei Cloud management console.

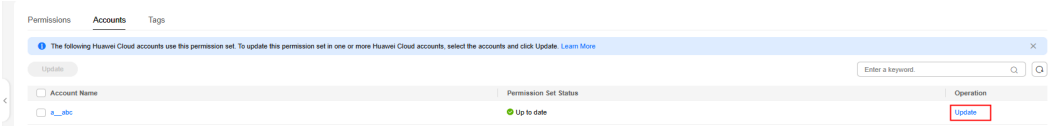
Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Multi-Account Permissions** > **Permission Sets**.

Step 4 In the permission set list, click the name of a permission set to view its details.

Step 5 On the **Accounts** tab, select the accounts whose permission set status is **Outdated** and click **Update** above the list. Alternatively, locate an account whose permission set status is **Outdated** and click **Update** in the **Operation** column.

Figure 3-10 Updating a permission set



Step 6 On the displayed page, confirm the details and click **Update** in the lower right corner of the page. After the update is complete, the permission set status of the account will be **Up to date**.

----End

3.2.3 Deleting a Permission Set

You can delete a permission set that is no longer needed. Before deleting a permission set, you must remove it from all accounts that use the permission set.

For details about how to remove a permission set from an account, see **Removing Access Permissions and Permission Sets**.

Deletion cannot be undone. Exercise caution when performing this operation.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Multi-Account Permissions** > **Permission Sets**.

Step 4 In the permission set list, locate the permission set and click **Delete** in the **Operation** column. In the displayed dialog box, click **OK**.

Figure 3-11 Deleting a permission set

----End

3.2.4 Managing Permission Set Tags

Tags

Tags help you to identify your cloud resources. When you have many cloud resources of the same type, you can use tags to classify them by dimension (for example, by purpose, owner, or environment).

IAM Identity Center allows you to add tags to permission sets. You can quickly search for and filter specific permission sets by tags to easily and efficiently identify and manage created permission sets.

After a permission set is created, you can add, modify, view, or delete tags on the permission set details page. You can add up to 20 tags for each permission set.

Constraints on Using Tags

- Each cloud resource can have a maximum of 20 tags.
- For each resource, each tag key must be unique, and each tag key can have only one tag value.

Procedure

You can add, edit, or delete tags of a permission set on the IAM Identity Center console.

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Multi-Account Permissions** > **Permission Sets**.

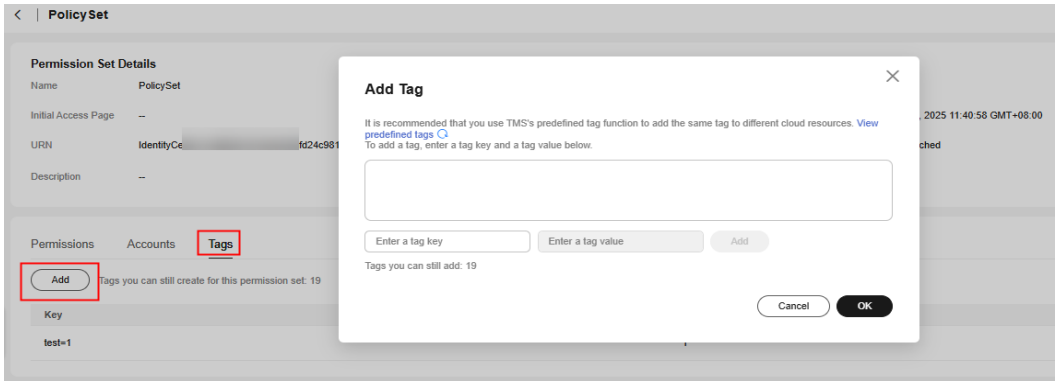
Step 4 In the permission set list, click the name of a permission set to view its details.

Step 5 On the **Tags** tab, click **Add**.

Step 6 In the displayed dialog box, enter a tag key and a tag value (optional), click **Add**, and then click **OK**.

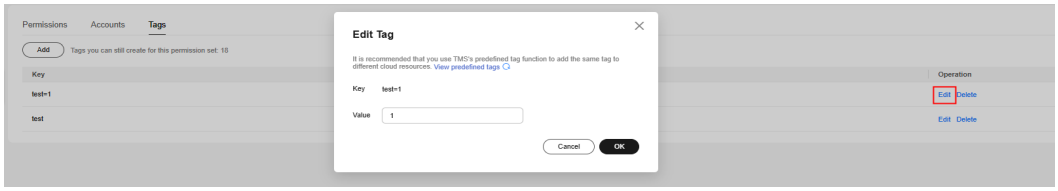
You can also select a predefined tag created on TMS from the drop-down list of the tag key. For more information about predefined tags, see .

Figure 3-12 Adding a tag



Step 7 Click **Edit** in the **Operation** column of the target tag. In the **Add Tag** dialog box, click **OK**.

Figure 3-13 Editing a tag



Step 8 Click **Delete** in the **Operation** column of the target tag. In the **Delete Tag** dialog box, click **OK**.

Figure 3-14 Deleting a tag

----End

3.3 Accounts

3.3.1 Associating Accounts with Users/Groups and Permission Sets

After IAM Identity Center users/groups and permission sets are created, you can associate one or more member accounts in your organization with the created users/groups and permission sets. This way, the IAM Identity Center users can access resources under the associated accounts after logging in to the system, and permissions included in the associated permission set can be granted to the resources.

Currently, you can only associate IAM Identity Center users/groups and permission sets with member accounts in your organization, rather than organizational units (OUs) or the whole organization.

The accounts can be either the management account or member accounts of your organization.

Procedure

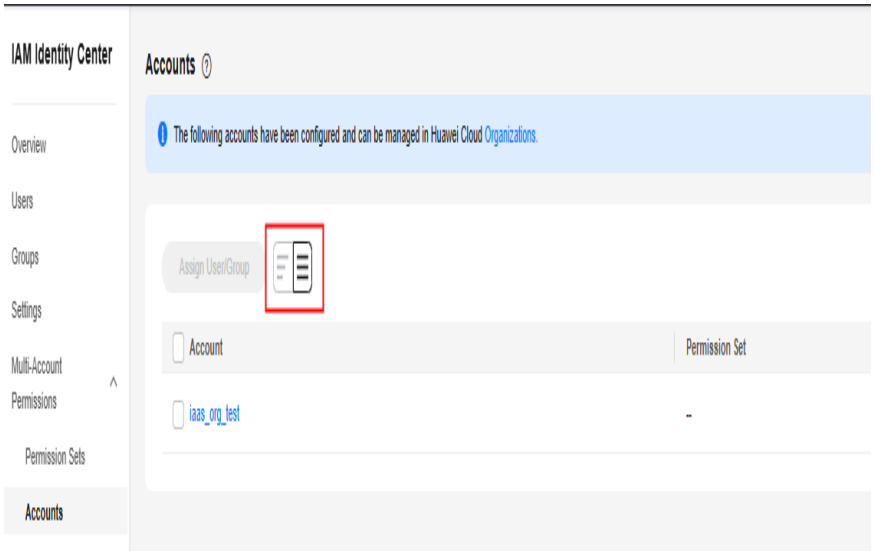
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Multi-Account Permissions** > **Accounts**.

By default, accounts are displayed in an organizational hierarchy structure. You can click  to switch to the list view.

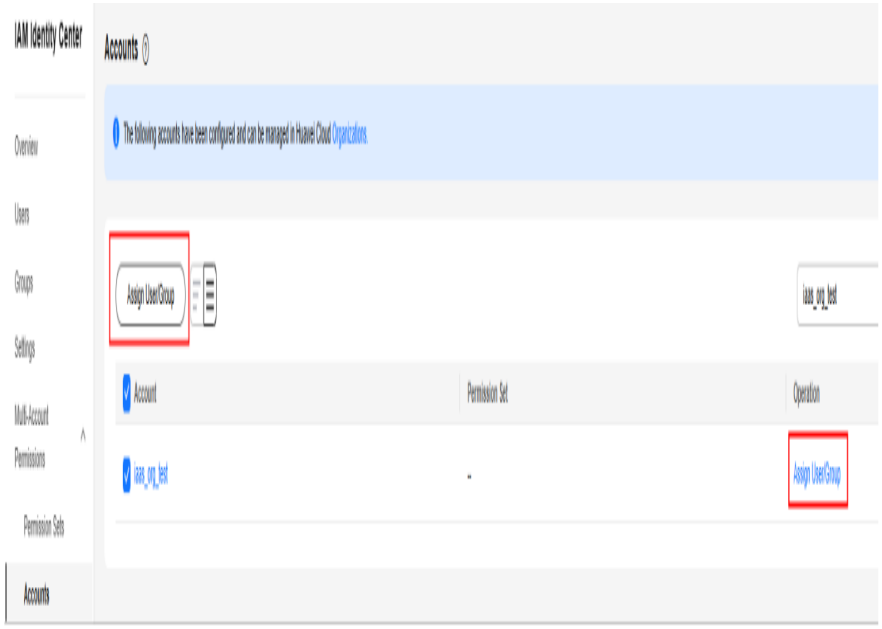
Figure 3-15 Account view



Step 4 Select one or more accounts from the account list and click **Assign User/Group** in the upper left corner.

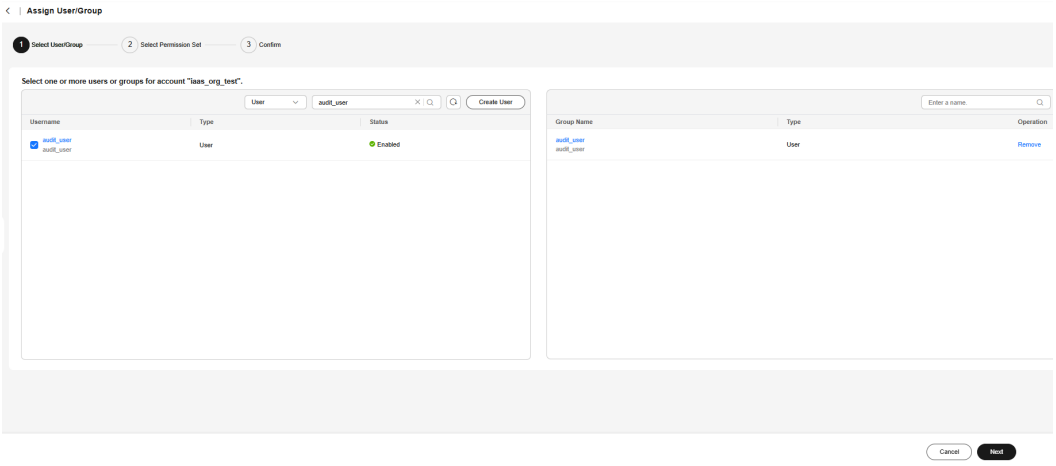
Alternatively, locate a target account and click **Assign User/Group** in the **Operation** column.

Figure 3-16 Selecting accounts



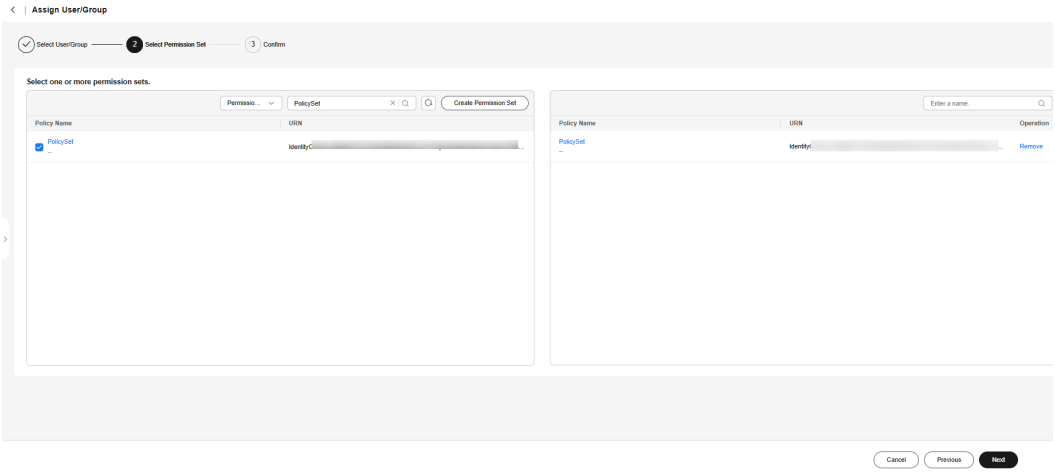
Step 5 In the **Select User/Group** step on the displayed page, select one or more users/groups and click **Next**.

Figure 3-17 Assigning users/groups



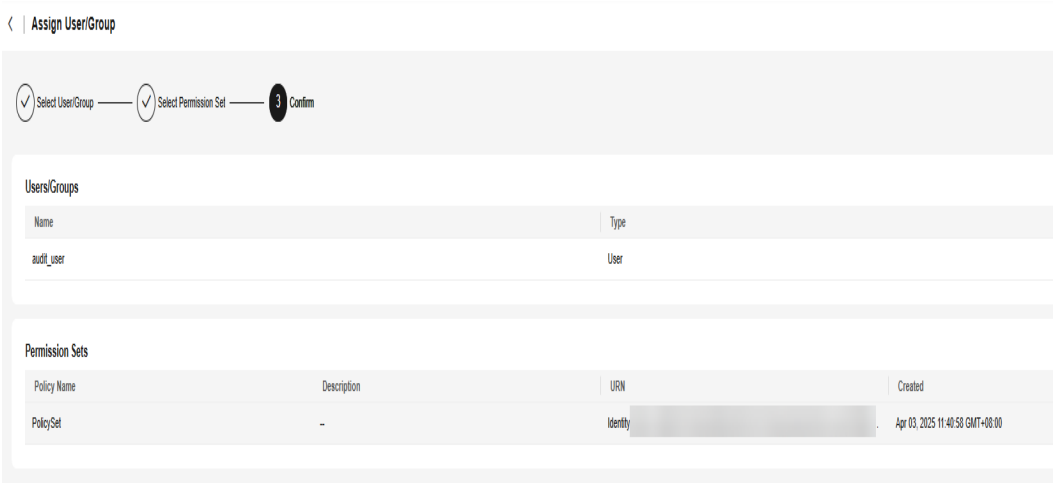
Step 6 In the **Select Permission Set** step, select one or more permission sets and click **Next**.

Figure 3-18 Selecting one or more permission sets



Step 7 In the **Confirm** step, confirm the configurations and click **OK**.

Figure 3-19 Confirming configurations



----End

3.3.2 Modifying Association with Users/Groups and Permission Sets

You can modify the association with users/groups and permission sets as needed.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Multi-Account Permissions** > **Accounts**.

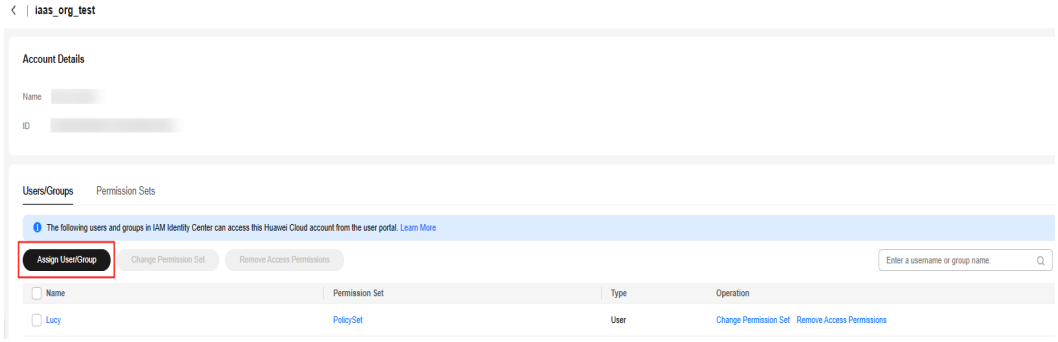
By default, accounts are displayed in an organizational hierarchy structure. You can click to switch to the list view.

Figure 3-20 Account view

Step 4 In the account list, click the name of a target account.

Step 5 On the **Users/Groups** tab, click **Assign User/Group** and modify the user/group assignments and associated permission sets. For details, see **Associating Accounts with Users/Groups and Permission Sets**.

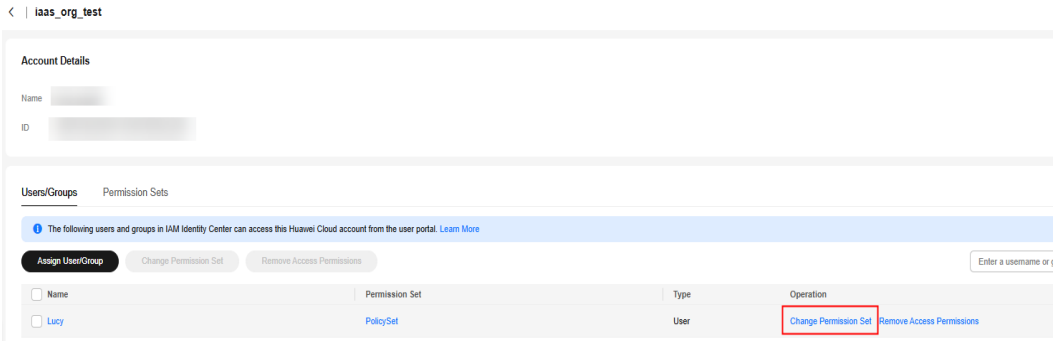
Figure 3-21 Assigning users/groups



Step 6 In the user/group list, select one or more users/groups and click **Change Permission Set** above the list. Alternatively, locate a user/group and click **Change Permission Set** in the **Operation** column.

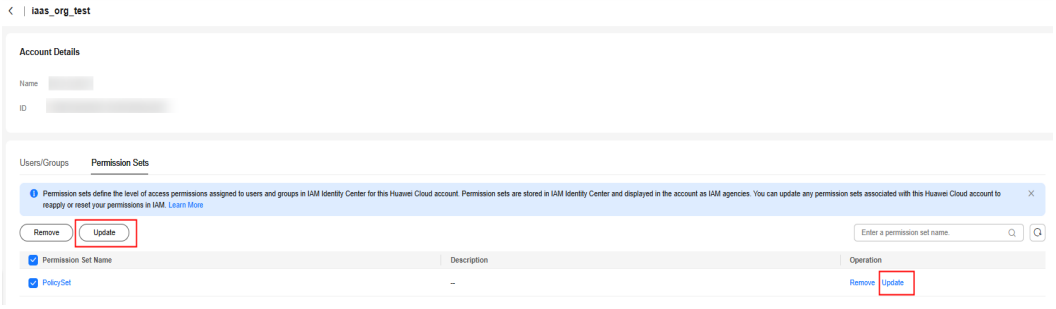
Step 7 On the displayed page, select or deselect permission sets in the permission set list and click **Confirm Change**.

Figure 3-22 Changing one or more permission sets



Step 8 (Optional) If the details or included policies of a permission set associated with the account are modified, click the **Permission Sets** tab, select one or more permission sets to be updated, and click **Update** above the list or in the **Operation** column.

Figure 3-23 Updating one or more permission sets



Step 9 On the displayed page, confirm the details and click **Update** in the lower right corner of the page.

----End

3.3.3 Removing Access Permissions and Permission Sets

You can remove access permissions or permission sets from an associated account.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Multi-Account Permissions** > **Accounts**.

By default, accounts are displayed in an organizational hierarchy structure. You can click to switch to the list view.

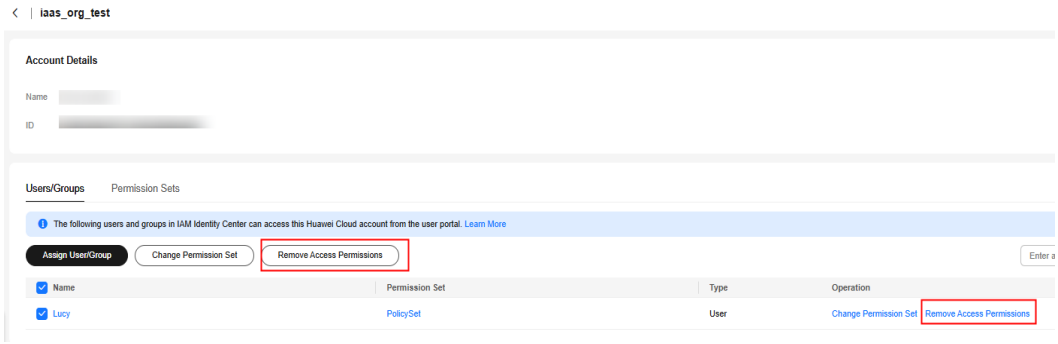
Figure 3-24 Account view

Step 4 In the account list, click the name of a target account.

Step 5 On the **Users/Groups** tab, select one or more users/groups and click **Remove Access Permissions** above the list. Alternatively, locate a target user/group and click **Remove Access Permissions** in the **Operation** column.

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

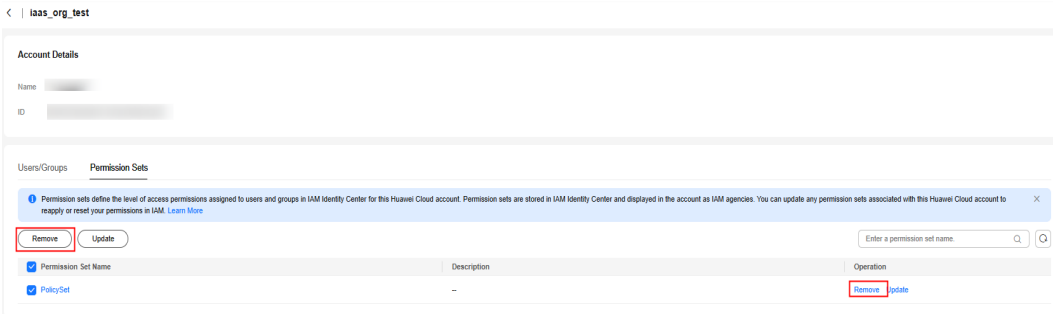
Figure 3-25 Removing access permissions



Step 7 On the **Permission Sets** tab, select one or more permission sets and click **Remove** above the list. Alternatively, locate a target permission set or click **Remove** in the **Operation** column.

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

Figure 3-26 Removing one or more permission sets



----End

3.4 Attribute-based Access Control (ABAC)

3.4.1 ABAC Overview and Configuration Process

Overview

Attribute-based Access Control (ABAC) is an authorization policy that defines permissions based on user attributes. You can use user attributes that come from different identity sources, such as IAM Identity Center or an external identity provider, to manage access to Huawei Cloud resources in IAM Identity Center. Using user attributes as tags simplifies the process of creating fine-grained permissions on Huawei Cloud and ensures that users can obtain only the Huawei Cloud resource permissions that match these tags.

For example, you can associate User_A and User_B with the same permission set, and then perform access control based on their display names. When User_A and User_B log in to the user portal to access the resources defined in the permission set, IAM Identity Center matches their display names with the resource tag values. They can access the resources only if their display names match the resource tag values. If User_A no longer needs to access some resources in this permission set, you can simply modify the resource tags to disable their access without updating any permission set configurations.

ABAC also helps reduce the number of permission sets you need to create and manage in IAM Identity Center. This is because users associated with the same permission set can now have unique permissions based on their user attributes. You can use these user attributes in a permission set to control access to Huawei Cloud resources and simplify permissions management.

Advantages of ABAC

- ABAC requires fewer permission sets: You do not have to create different permission sets for different users, so the number of permission sets and the complexity of permissions management can be reduced.
- ABAC helps the team change and grow quickly: You can tag resources appropriately when creating resources. Then the system automatically grants permissions to the created resources based on user attributes.

- Use employee attributes in the enterprise directory through ABAC: You can use the existing employee attributes of any identity source configured in IAM Identity Center to make access control decisions on Huawei Cloud.

Configuration Process

The following table lists the operations required for preparing Huawei Cloud resources and configuring IAM Identity Center for ABAC access control. To use ABAC, you need to perform all the operations listed in the table.

Table 3-2 ABAC configuration process

Procedure	Description	Reference
Adding tags to a resource	To perform ABAC in IAM Identity Center, you first need to add tags to the target resources. The resource tag value must be consistent with the user attribute, so that the match is successful in permissions policies and the access control policies can be applied. For example, if you want to use the username attribute for access control and the username is **User1**, the resource tag value must also be **User1**.	**Adding Tags to Cloud Resources**
Configuring the identity source	You can choose IAM Identity Center or an external identity provider as your identity source. The user attributes of both identity sources can support ABAC. You can switch between the two identity sources in IAM Identity Center.	**Changing the Identity Source**
Enabling and configuring ABAC in IAM Identity Center	• IAM Identity Center as identity source: Enable ABAC on the IAM Identity Center console and add user attributes for configuring ABAC. • External identity provider as identity source: Enable ABAC on the IAM Identity Center console, and then configure ABAC in IAM Identity Center or the external identity provider.	**Enabling and Configuring Access Control Attributes**

Procedure	Description	Reference
Creating a permissions policy for ABAC	You can create a custom identity policy in the permission set and use access control attributes to create ABAC-related rules to allow users to access resources only with matching tags. The user attributes you added in the previous step are used as tags for access control decisions. You can use the "PrincipalTag/key" condition key to reference the access control attributes in the permission policy.	**Creating Permissions Policies for ABAC**
Associating accounts with users/groups and permission sets	You can associate related accounts and IAM Identity Center users with the permission set created in the previous step. In this way, when a user logs in to the user portal to access resources under the associated accounts, they can only access resources whose tags match the user attributes.	**Associating Accounts with Users/Groups and Permission Sets**
Logging in as an IAM Identity Center user and accessing resources	After the preceding steps are complete, the IAM Identity Center user associated with related accounts and permission sets can log in to the user portal and obtain the resource access permissions based on the matched user attributes.	**Logging In as an IAM Identity Center User and Accessing Resources**

3.4.2 Enabling and Configuring Access Control Attributes

Scenarios

To perform ABAC in an identity source, you need to enable access control in IAM Identity Center and add user attributes that need to be used in permission set policies to control user access to resources. The user attributes that can be added include basic information, contact information, work-related information, and address information. For details about the user attributes that support ABAC, see **Supported User Attributes**.

For example, if you want to use the username to assign their access to resources in the organization, you can add the username attribute on the **Access Control**

Attributes tab for ABAC. Then, you can add a custom identity policy to the permission set in IAM Identity Center. This policy grants access permissions to a user only when their username matches the tag value you assigned to the organizational resources. For details about ABAC-related custom policies, see **Creating Permissions Policies for ABAC**.

The differences between performing ABAC on IAM Identity Center and on external identity providers are as follows:

- IAM Identity Center: You need to add the attributes for performing ABAC on the **Access Control Attributes** tab of IAM Identity Center.
- External identity provider: You can add the attributes in either of the following ways.
  - Add the ABAC attributes in the external identity provider. You can configure an external identity provider to send attributes through SAML assertions. In this case, IAM Identity Center obtains the attribute keys and attribute values passed from the external identity provider for policy evaluation. For details, see the external identity provider documentation.

    NOTE

    Attributes passed through SAML assertions are invisible on the **Access Control Attributes** tab of IAM Identity Center. You must learn about them in advance and add them to access control rules when creating permissions policies.
  - Configure ABAC attributes on the **Access Control Attributes** tab of IAM Identity Center. If the ABAC attributes configured in IAM Identity Center are the same as those configured in the external identity provider, the former is preferentially used for access control decisions.

This section only describes the operations performed on the IAM Identity Center console. For the operations performed on the external identity provider, see their documentation.

Enabling Access Control Attributes

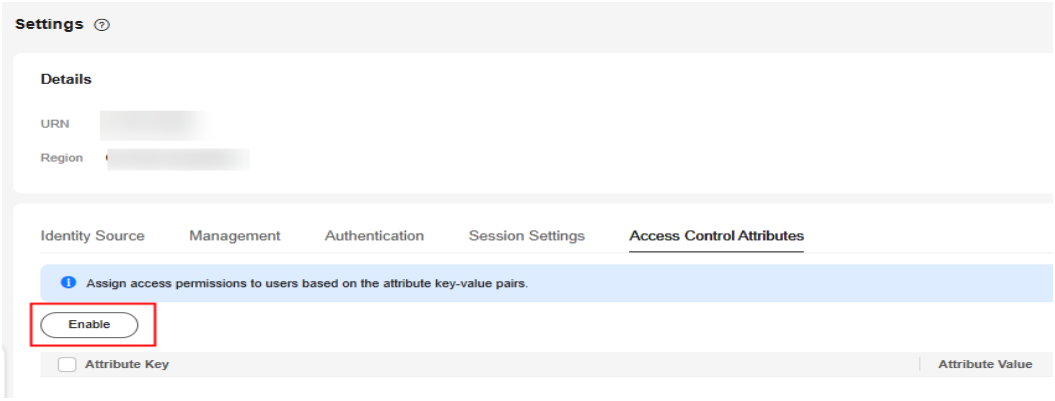
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 Click **Enable** on the **Access Control Attributes** tab.

Figure 3-27 Enabling access control attributes



----End

Configuring Access Control Attributes

After access control attributes are enabled, you need to add attribute keys and attribute values for access control. A maximum of 20 attributes can be added.

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 Click **Add** on the **Access Control Attributes** tab.

Step 5 In the displayed dialog box, add attribute keys and attribute values of the user for access control.

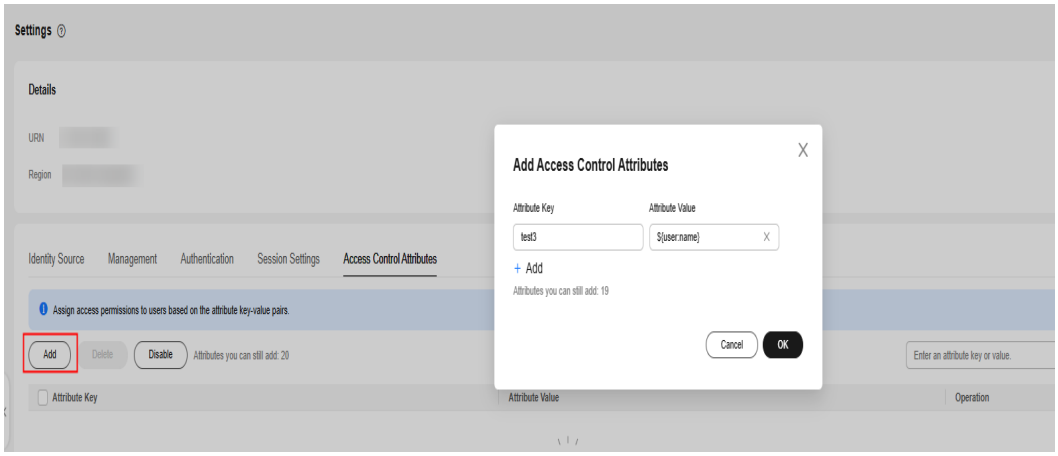
- **Attribute Key**: specifies the name of a user attribute and can be used in permissions policies. Only a single value is supported.

  You can enter any name, which will be used when you define custom identity policies in the permission set. For example, if you set the attribute key to User_A, the **PrincipalTag** condition key in the custom identity policy must also be set to User_A, that is, **g:ResourceTag/*tag-key*": "${g:PrincipalTag/User_A}**.

- **Attribute Value**: specifies the type of a user attribute. You can select a user attribute type from the drop-down list box.

  For example, if you select **${user:name}**, then the username is used for access control. During authorization, the username must match the resource tag value. For details about the supported user attributes, see **Supported User Attributes**.

Figure 3-28 Adding access control attributes



Step 6 After the configuration is complete, click **OK**.

Now that you have enabled and configured access control attributes, you need to create custom identity policies of ABAC in the permission set by referring to **Creating Permissions Policies for ABAC**.

----End

Editing or Deleting Access Control Attributes

After the access control attributes are added, you can modify or delete them at any time as required.

Step 1 Log in to the Huawei Cloud management console.

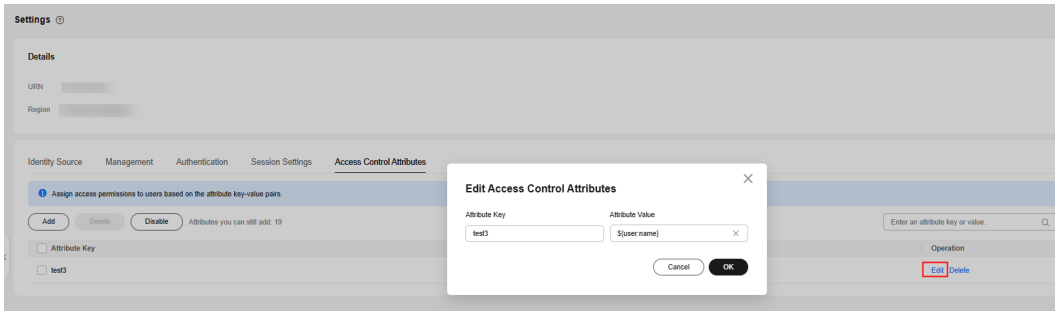
Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 On the **Access Control Attributes** tab, click **Edit** in the **Operation** column of the list.

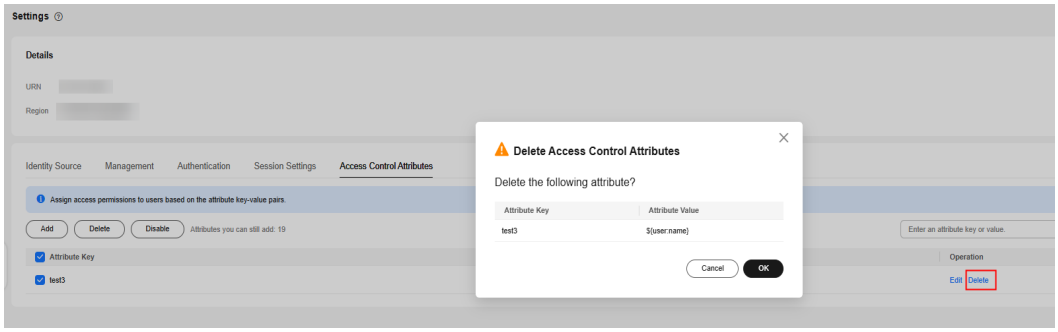
Step 5 In the displayed dialog box, modify the attribute key or value and click **OK**.

Figure 3-29 Editing access control attributes



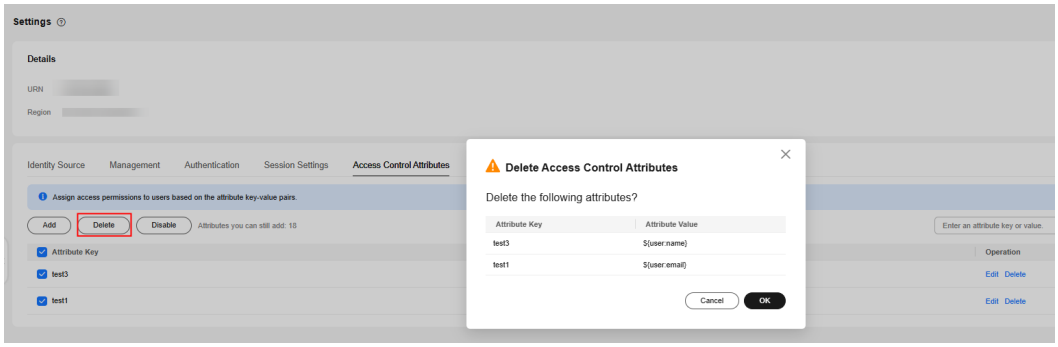
Step 6 Click **Delete** in the **Operation** column of the row that contains the target access control attribute. In the displayed dialog box, click **OK**.

Figure 3-30 Deleting an access control attribute



Step 7 Select multiple access control attributes to be deleted from the list and click **Delete** above the list. In the displayed dialog box, click **OK**.

Figure 3-31 Batch deleting access control attributes



----End

Disabling Access Control Attributes

If you no longer need to use the ABAC function, you can disable it at any time. This operation will delete all configured attributes and cannot be restored. Exercise caution when performing this operation.

Step 1 Log in to the Huawei Cloud management console.

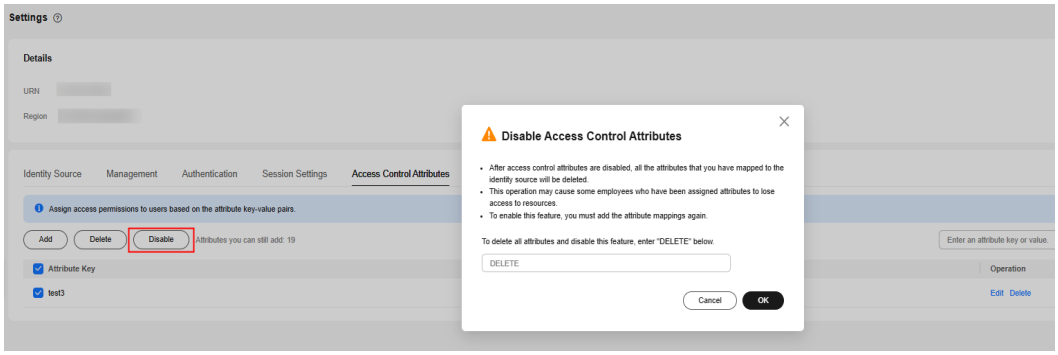
Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 On the **Access Control Attributes** tab, click **Disable**.

Step 5 In the displayed dialog box, read the information carefully. After confirmation, enter **DELETE** and click **OK**.

Figure 3-32 Disabling access control attributes



----End

3.4.3 Creating Permissions Policies for ABAC

Overview

After you add tags to resources and enable and configure access control attributes in IAM Identity Center, you need to add attribute-based access control rules to custom identity policies of the permission set. With the **PrincipalTag** conditional key, you can create access control rules using access control attributes in a permission set. That is, enter **g:ResourceTag/*tag-key*": "${g:PrincipalTag/*tag-key*}** in the **Condition** element of the policy statement.

- **g:ResourceTag/*tag-key***: Global condition key, which specifies the resource tag key. After tagging a resource, you need to enter the resource tag key in this condition key, that is, replace ***tag-key*** with a specific resource tag key.
- **g:PrincipalTag/*tag-key***: Global condition key, which specifies the attribute key of an access control attribute. After enabling and adding access control attributes, you need to enter the attribute key of an access control attribute in the condition key, that is, replace ***tag-key*** with a specific attribute key.

After the preceding access control rules are configured, the permissions policy verifies the resource tag value and attribute value based on the specified resource tag key and attribute key. Only users whose resource tag value matches the attribute value can obtain the resource access permissions defined in the permission set.

Example Policies

For details about how to create a permission set, see **Creating a Permission Set**. The following describes how to add attribute-based access control rules to custom identity policies in permission sets and gives some example policies.

For example, if you select the **OrganizationsFullAccessPolicy** system policy when creating a permission set, users associated with the permission set have all permissions of Organizations. If you do not want some users to have permission to delete a specified organization unit (OU), you can add the following policy content to custom identity policies of the permission set to prevent these users from deleting the specified OUs.

The condition key determines the users and resources on which the custom identity policy takes effect. In the example, the condition key indicates that the

resource tag key is **orgtag1** and the access control attribute key is **User_A**. During policy evaluation, the tag value of **orgtag1** is matched with the attribute value of **User_A**. For example, if you set the tag value of **orgtag1** to **test1** and the attribute value of **User_A** to **${user:name}**, only the user **test1** can obtain the permissions defined in this policy.

For complex authorization scenarios, such as multi-user and multi-resource authorization, refer to the following:

- If you want to use this policy to grant a user the permissions needed to access multiple resources, you only need to attach the same tag to these resources.
- If you want to use this policy to control multiple users' access to a resource, you can attach multiple tags to the resource and enter multiple condition keys in the custom identity policy of the permission set to map the attributes of multiple users.
- If you want to use this policy to control multiple users' access to multiple resources, you can add tags with the same tag key but different tag values to multiple resources to map the attributes of multiple users.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "organizations:ous:delete"
      ],
      "Condition": {
        "StringEquals": {
          "g:ResourceTag/orgtag1": "${g:PrincipalTag/User_A}"
        }
      }
    }
  ]
}
```

3.4.4 Supported User Attributes

You can choose IAM Identity Center or an external identity provider as your identity source. The following table lists the user attributes that support ABAC for the two identity sources. These user attributes can be selected during the configuration of access control attributes. These attribute values include basic information, contact information, work-related information, and address information of users. You can select these user attributes and assign attribute keys to them for access control decisions when performing ABAC.

If you use an external identity provider as the identity source, you can configure user attributes for performing ABAC in both IAM Identity Center and the external identity provider. If the ABAC attribute keys configured in IAM Identity Center are the same as those configured in the external identity provider, the former is preferentially used for access control decisions.

Table 3-3 Supported user attributes

Identity Source	User Attribute
IAM Identity Center	${user:email}

Identity Source	User Attribute
	${user:familyName}
	${user:givenName}
	${user:middleName}
	${user:name}
	${user:displayName}
External identity provider	${path:userName}
	${path:name.familyName}
	${path:name.givenName}
	${path:displayName}
	${path:nickName}
	${path:emails[primary eq true].value}
	${path:addresses[type eq "work"].streetAddress}
	${path:addresses[type eq "work"].locality}
	${path:addresses[type eq "work"].region}
	${path:addresses[type eq "work"].postalCode}
	${path:addresses[type eq "work"].country}
	${path:addresses[type eq "work"].formatted}
	${path:phoneNumbers[type eq "work"].value}
	${path:userType}
	${path:title}
	${path:locale}
	${path:timezone}
	${path:enterprise.employeeNumber}
	${path:enterprise.costCenter}
	${path:enterprise.organization}
	${path:enterprise.division}
	${path:enterprise.department}
	${path:enterprise.manager.value}

4 Identity Source Management

4.1 Changing the Identity Source

IAM Identity Center provides identity federation based on Security Assertion Markup Language (SAML). This function allows users in your enterprise management system to access Huawei Cloud through single sign-on (SSO). For details about IAM IdPs, see **Identity Providers**.

IAM Identity Center works with SAML 2.0-based external identity provider systems, such as Microsoft Azure Active Directory (AD) or Okta. The implementation is as follows:

- IAM Identity Center can connect to external identity provider systems via SAML 2.0.
- IAM Identity Center automatically provisions users from SCIM-compliant identity providers. The administrator can manage users in external identity providers. User details can be automatically synchronized to IAM Identity Center without manual intervention.
- IdP users can use their existing accounts and passwords to log in to the portal and then go to Huawei Cloud to access resources of the Huawei Cloud account.

You can choose IAM Identity Center or an external identity provider as your identity source. You can change your identity source in IAM Identity Center.

Changing to External Identity Provider

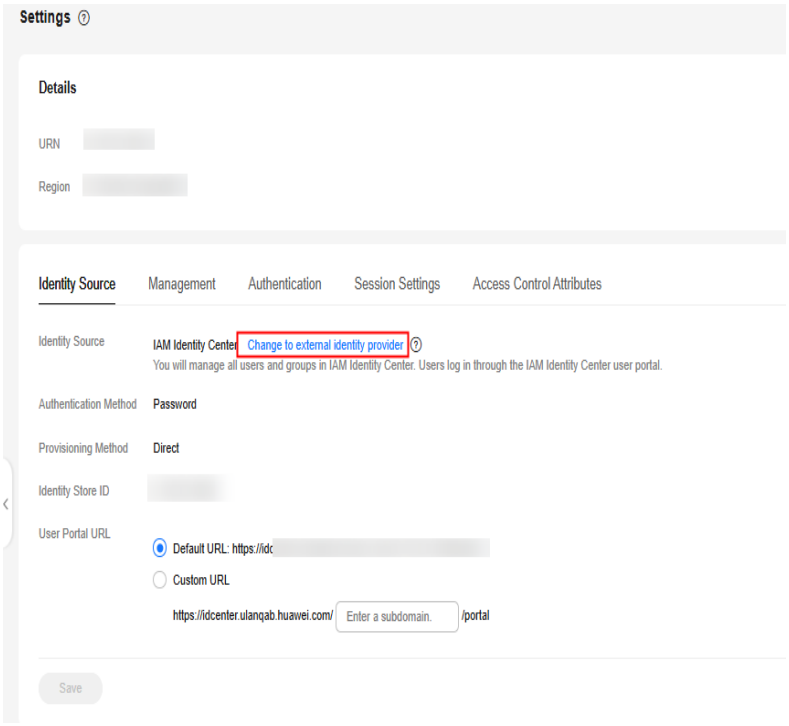
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 On the **Identity Source** tab, click **Change to external identity provider** in the **Identity Source** row.

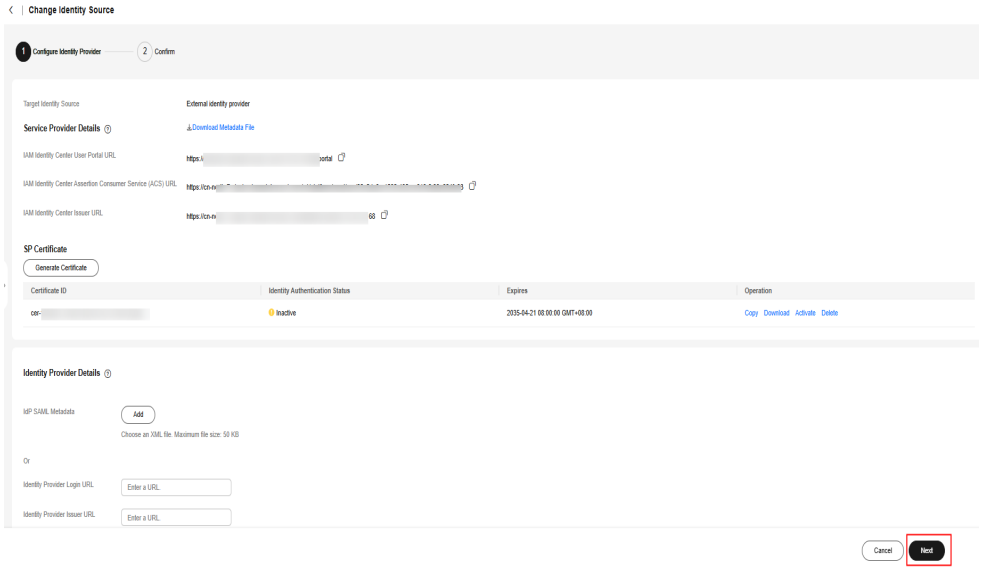
Figure 4-1 Changing to external identity provider



Step 5 In the **Configure Identity Provider** step on the displayed page, configure required information and click **Next**.

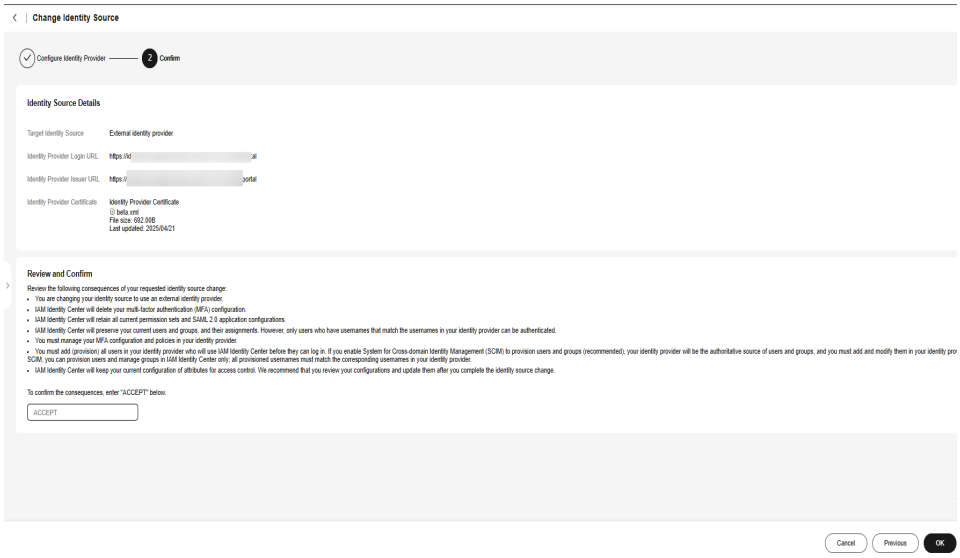
- Service provider details
  - Click **Download Metadata File** and save the downloaded file on your system. The IAM Identity Center SAML metadata file is required by your external identity provider.
  - If you do not have a service provider (SP) SAML metadata file, you can use the default SP information. If you need to use signed SAML authentication requests later, you can manually generate an SP certificate and activate it.
- Identity provider details
  - In the **IdP SAML Metadata** row, click **Select File** and upload the SAML metadata file downloaded from your external identity provider. This metadata file contains the certificate used to trust messages that are sent from the identity provider.
  - If you did not obtain the IdP SAML metadata file, enter the IdP login URL and IdP issuer URL, and upload the IdP certificate.

Figure 4-2 Configuring an identity provider



Step 6 In the **Confirm** step, review and confirm the change. After you read the disclaimer and are ready to proceed, enter **ACCEPT** in the text box and click **OK** in the lower right corner of the page.

Figure 4-3 Confirming the change of the identity source



NOTE

After the identity source is changed to an external identity provider, the system supports SAML 2.0-based identity federation as well as manual and automatic SCIM provisioning. For details, see **Configuring an External Identity Provider**.

----End

Changing to IAM Identity Center

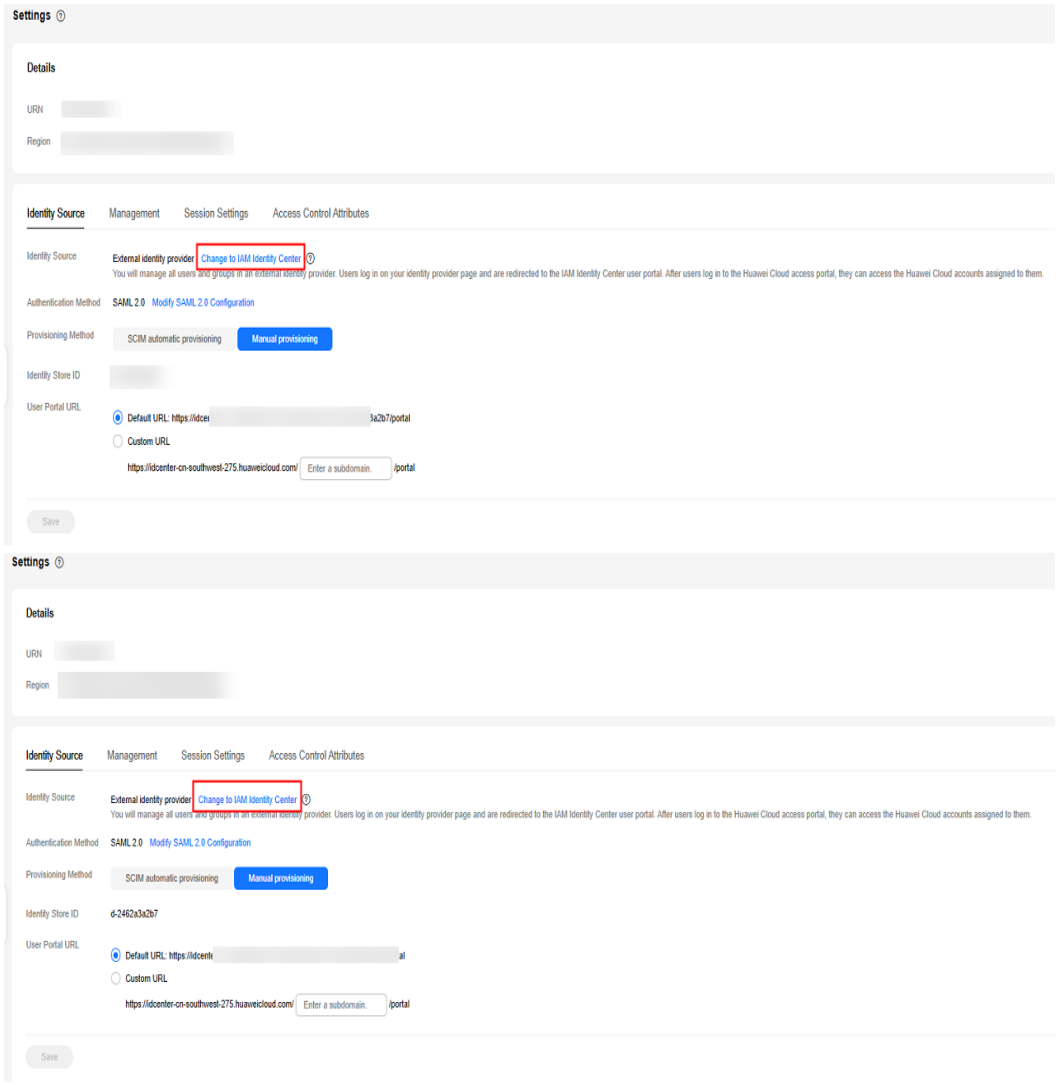
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

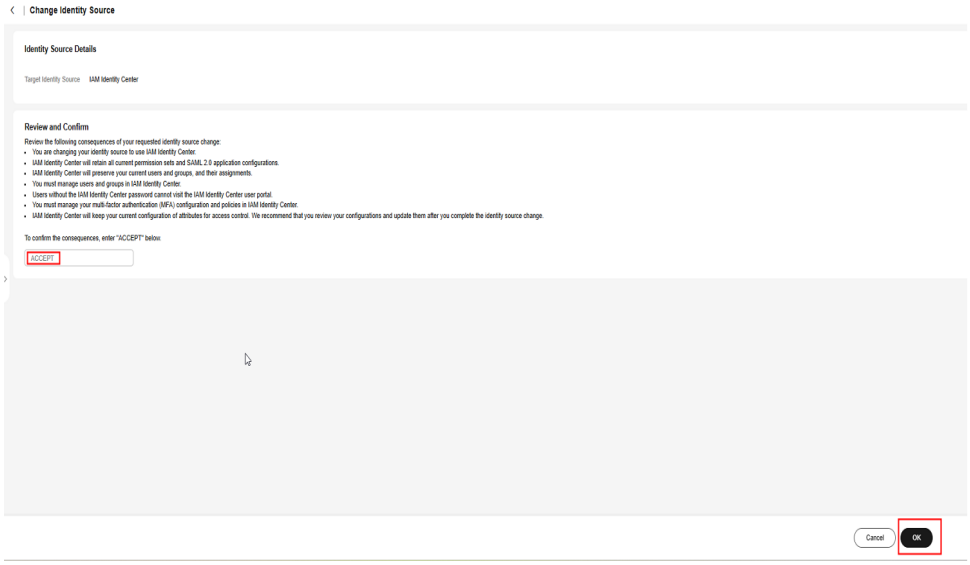
Step 4 On the **Identity Source** tab, click **Change to IAM Identity Center** in the **Identity Source** row.

Figure 4-4 Changing to IAM Identity Center



Step 5 Review and confirm the change. After you read the disclaimer and are ready to proceed, enter **ACCEPT** in the text box and click **OK** in the lower right corner of the page.

Figure 4-5 Confirming the change of the identity source



----End

4.2 Customizing User Portal URL

After you enable IAM Identity Center, a unique user portal URL is automatically generated. You can customize the URL only once. After the URL is changed, it cannot be modified any longer.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

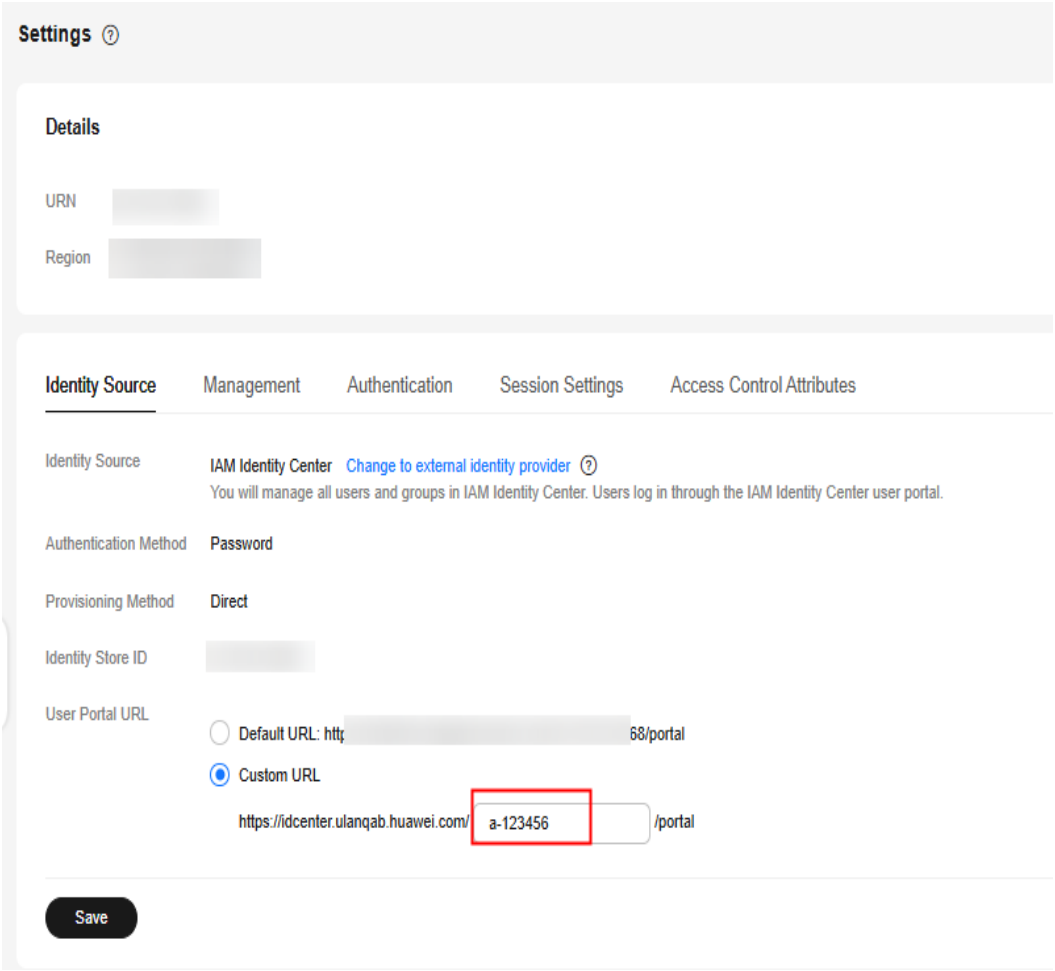
Step 3 Choose **Settings** in the navigation pane.

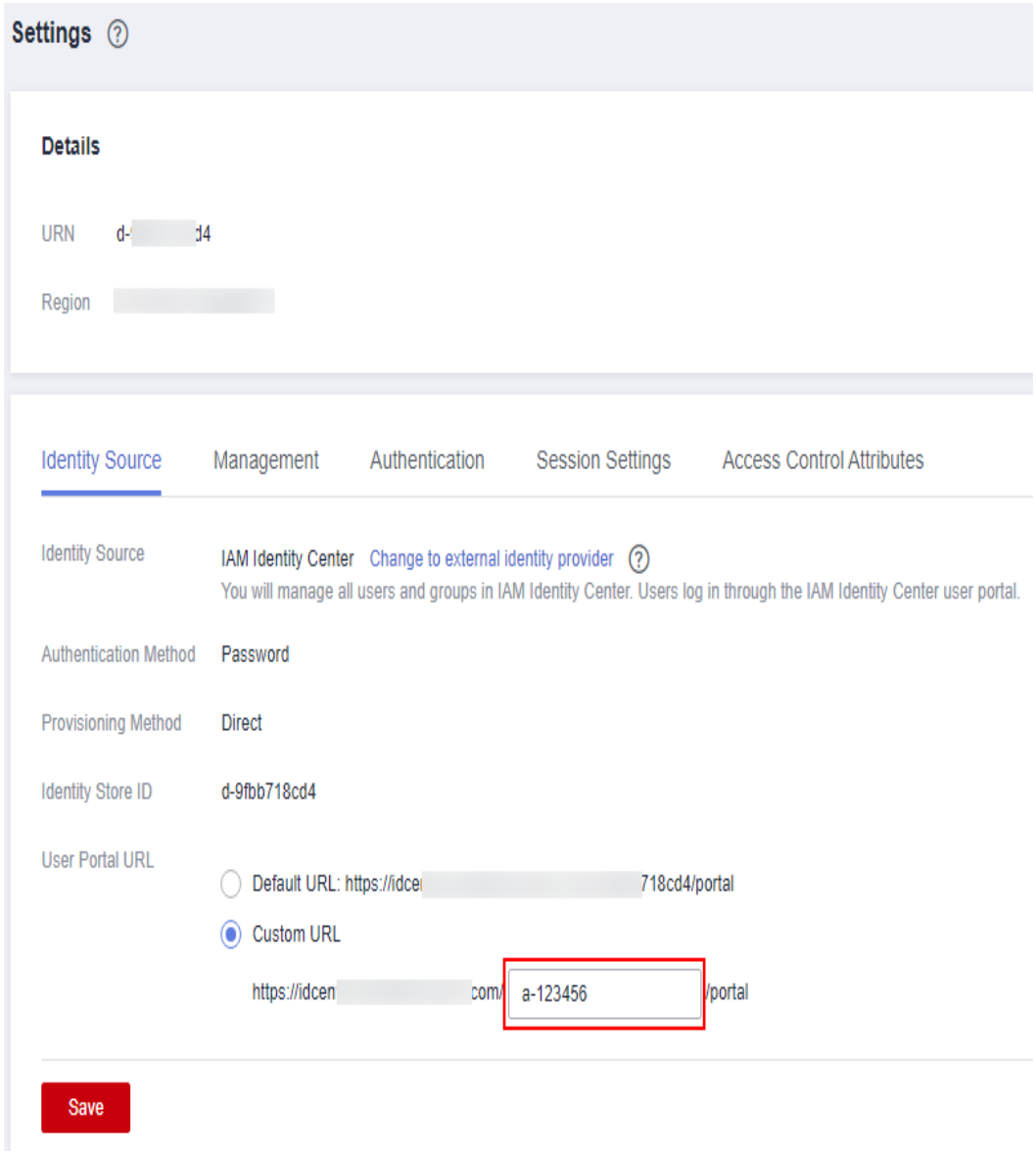
Step 4 On the **Identity Source** tab, select **Custom URL** for **User Portal URL**.

Step 5 Enter the user-defined subdomain and click **Save**.

A custom URL must contain 1 to 62 characters, including only letters, digits, and hyphens (-), and it must start and end with a letter or digit. It cannot start with **d-**.

Figure 4-6 Customizing the user portal URL





----End

4.3 Configuring an External Identity Provider

4.3.1 Overview of External Identity Providers

SAML 2.0

SAML 2.0 is an XML-based protocol that uses securityTokens 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 federated identity authentication in compliance with SAML

2.0. To successfully federate existing users to HUAWEI CLOUD, ensure that your enterprise IdP is compatible with this protocol.

IAM Identity Center supports identity federation with Security Assertion Markup Language (SAML). IAM Identity Center adds SAML IdP capabilities to either your IAM Identity Center identity store or external identity provider (IdP) applications. Users can then single sign-on into services that support SAML, including the Huawei Cloud console and third-party applications. The SAML protocol however does not provide a way to query the IdP to learn about users and groups, so you must make IAM Identity Center aware of those users and groups by provisioning them into IAM Identity Center.

SCIM

IAM Identity Center supports the System for Cross-domain Identity Management (SCIM) v2.0 standard. SCIM keeps your IAM Identity Center identities in sync with identities from your IdP. This includes any provisioning, updates, and deprovisioning of users between your IdP and IAM Identity Center. For details about how to implement SCIM, see **Enabling or Disabling SCIM Automatic Provisioning**.

4.3.2 Modifying SAML 2.0 Configuration

After the identity source is changed to an external identity provider, you can modify the SAML 2.0 configuration at any time, including modifying the provider information and modifying, activating, and deleting certificates.

Modifying SP Information

Step 1 Log in to the Huawei Cloud management console.

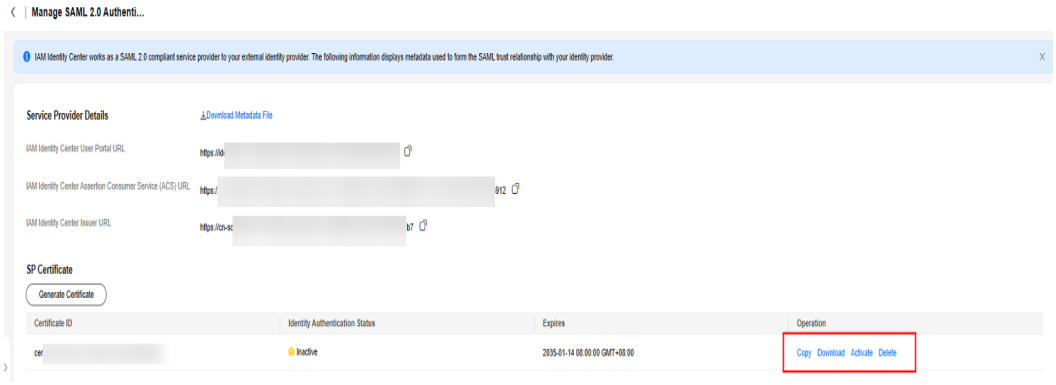
Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 On the **Identity Source** tab, click **Modify SAML 2.0 Configuration** in the **Authentication Method** row.

Step 5 On the displayed page, you can download and view the certificates and generate, activate, or delete the certificates in the **SP Certificate** area.

Figure 4-7 Modifying SP information



----End

Modifying IdP Information

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

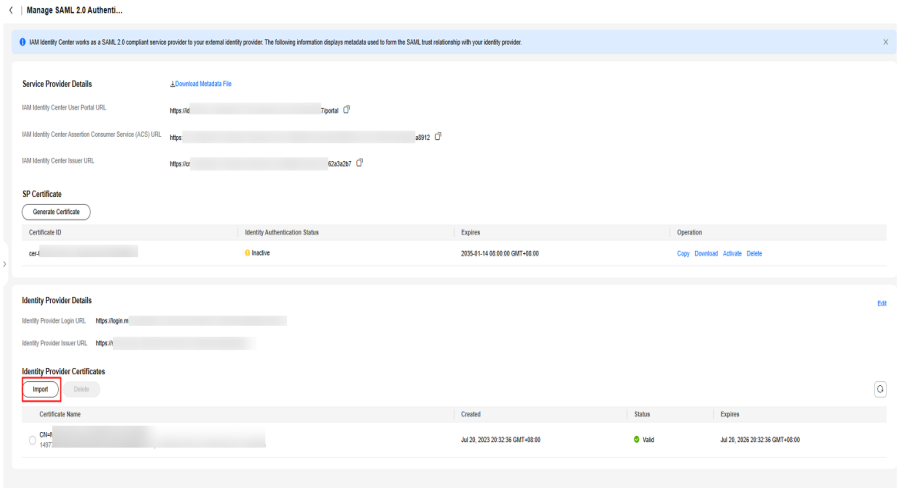
Step 4 On the **Identity Source** tab, click **Modify SAML 2.0 Configuration** in the **Authentication Method** row.

Step 5 On the displayed page, in the **Identity Provider Details** area, click **Edit**.

Step 6 Modify the identity provider login URL and identity provider issuer URL, and click **Save**.

Step 7 In the **Identity Provider Certificates** area, import or delete certificates by referring to **Rotating Certificates**.

Figure 4-8 Modifying IdP information



----End

4.3.3 Enabling or Disabling SCIM Automatic Provisioning

IAM Identity Center supports automatic provisioning (synchronization) of user and group information from your IdP into IAM Identity Center using the SCIM v2.0 protocol. When you configure SCIM synchronization, you create a mapping of your IdP user attributes to the named attributes in IAM Identity Center. This causes the expected attributes to match between IAM Identity Center and your IdP. You configure this connection in your IdP using your SCIM endpoint for IAM Identity Center and a bearer token that you create in IAM Identity Center.

This section includes the following content:

- **Enabling Automatic Provisioning**
- **Disabling Automatic Provisioning**
- **Generating or Deleting an Access Token**

Enabling Automatic Provisioning

Automatic provisioning is available only when the identity source is configured as an external identity provider.

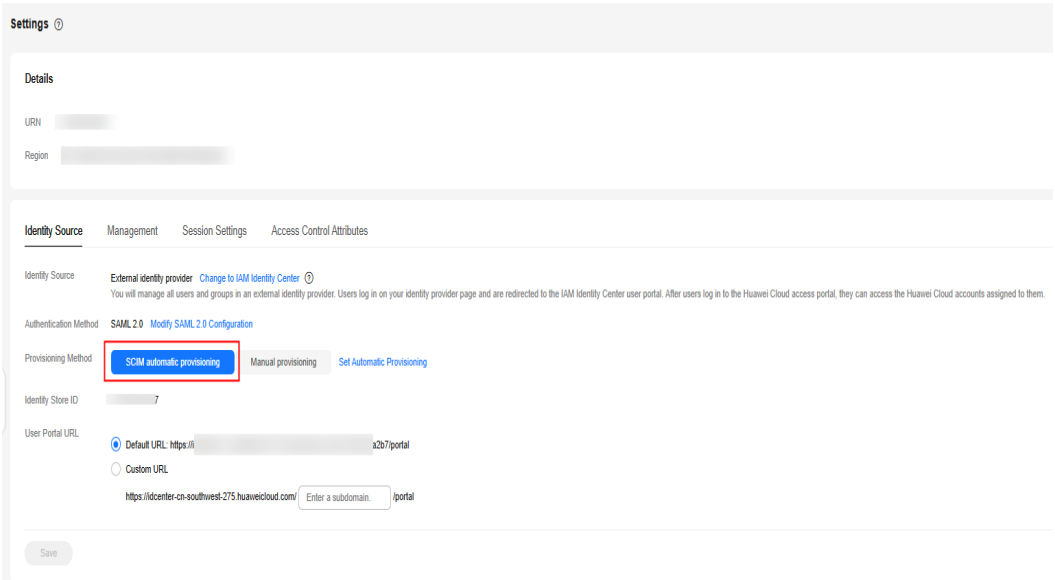
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 On the **Identity Source** tab, select **SCIM automatic provisioning** for **Provisioning Method** and click **Save**.

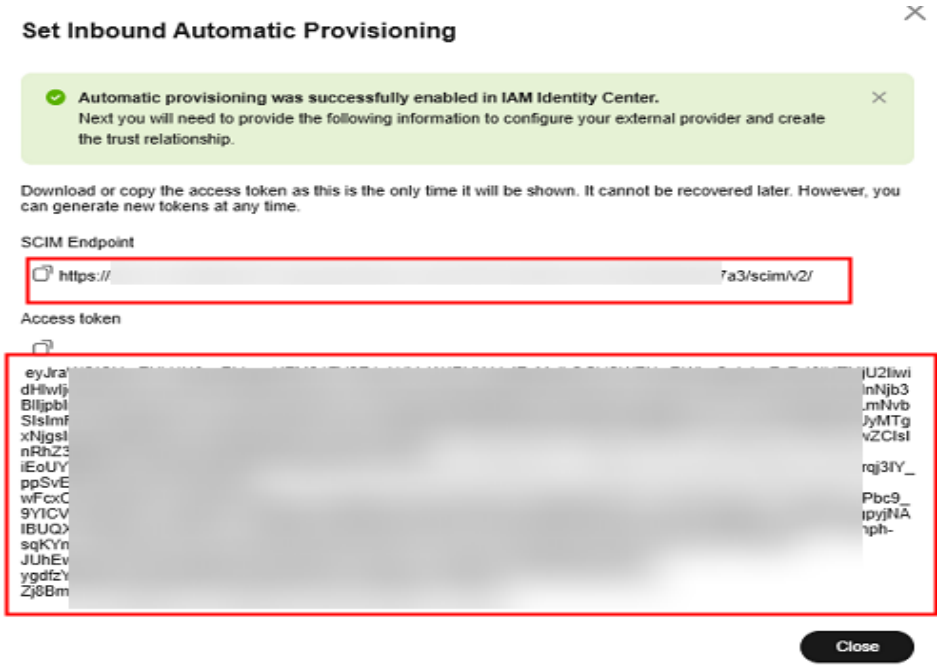
Figure 4-9 Enabling SCIM automatic provisioning



Step 5 In the displayed dialog box, copy the SCIM endpoint and access token. You will need this information when configuring provisioning in your IdP.

The access token is displayed only once and cannot be viewed later. However, you can generate new tokens at any time. For details, see **Generating or Deleting an Access Token**.

Figure 4-10 Inbound automatic provisioning



Step 6 Click **Close**.

----End

Disabling Automatic Provisioning

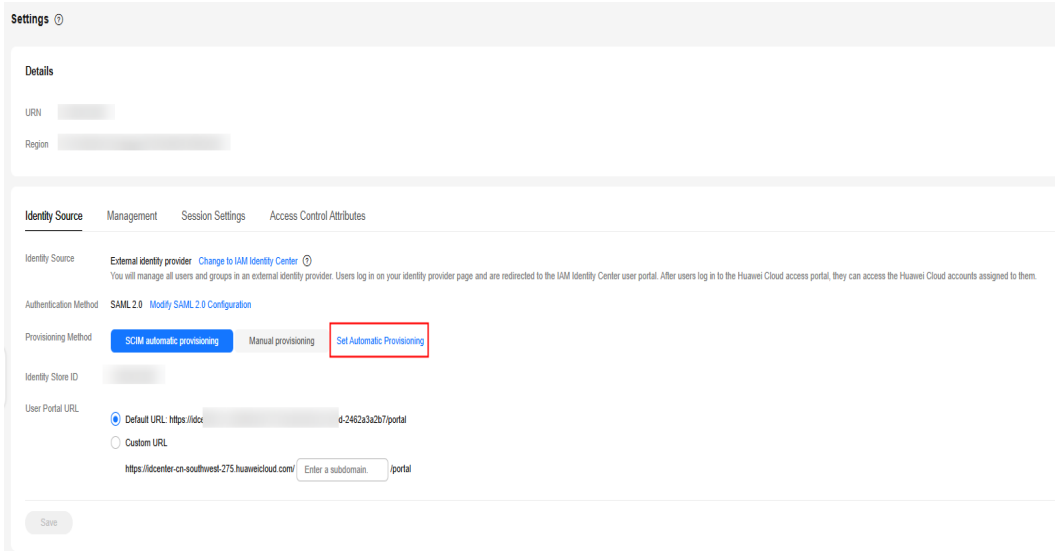
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 On the **Identity Source** tab, select **Set Automatic Provisioning** for **Provisioning Method**.

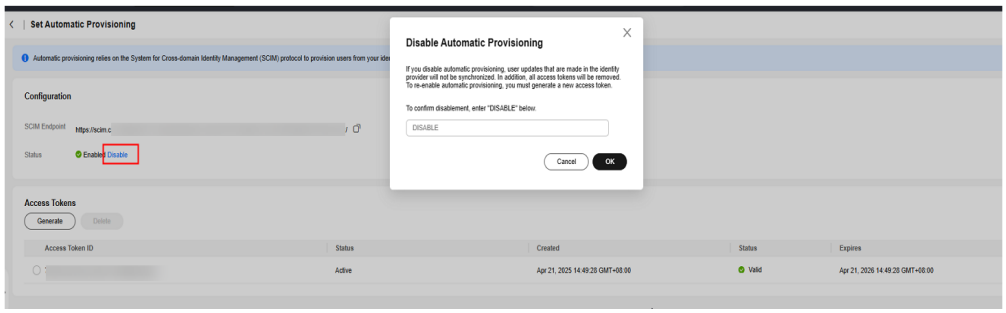
Figure 4-11 Setting automatic provisioning



Step 5 In the **Configuration** area, click **Disable** in **Status**. In the displayed dialog box, enter **DISABLE** and click **OK**.

After you disable automatic provisioning, user updates that are made in the identity provider will not be synchronized. In addition, all access tokens will be removed. To re-enable automatic provisioning, you must generate a new access token.

Figure 4-12 Disabling automatic configuration



----End

Generating or Deleting an Access Token

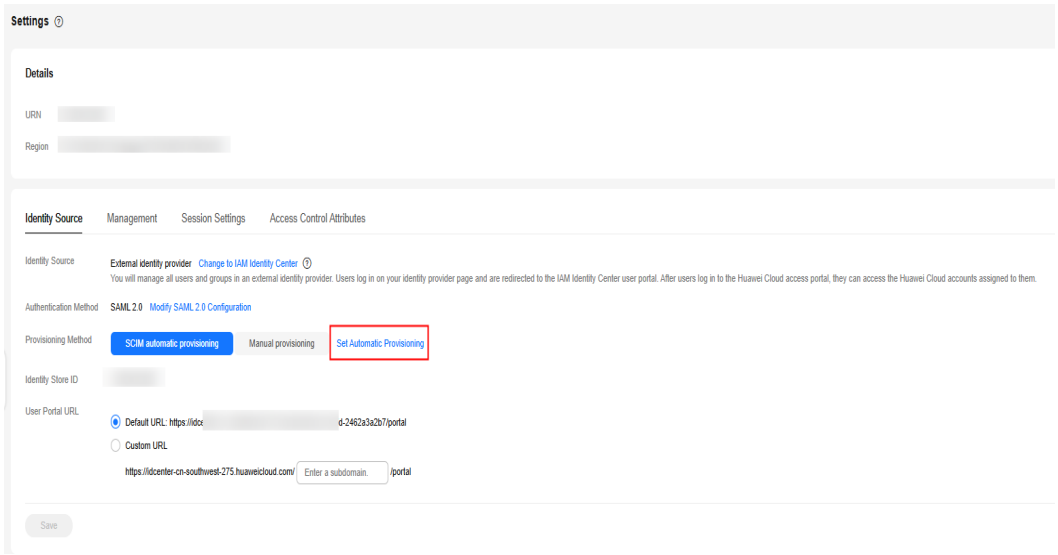
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

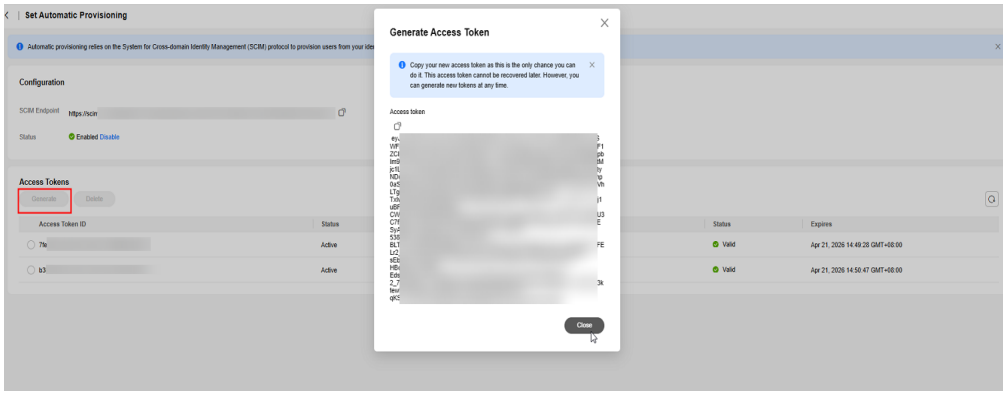
Step 4 On the **Identity Source** tab, select **Set Automatic Provisioning** for **Provisioning Method**.

Figure 4-13 Setting automatic provisioning



Step 5 On the displayed page, in the **Access Tokens** area, click **Generate**.

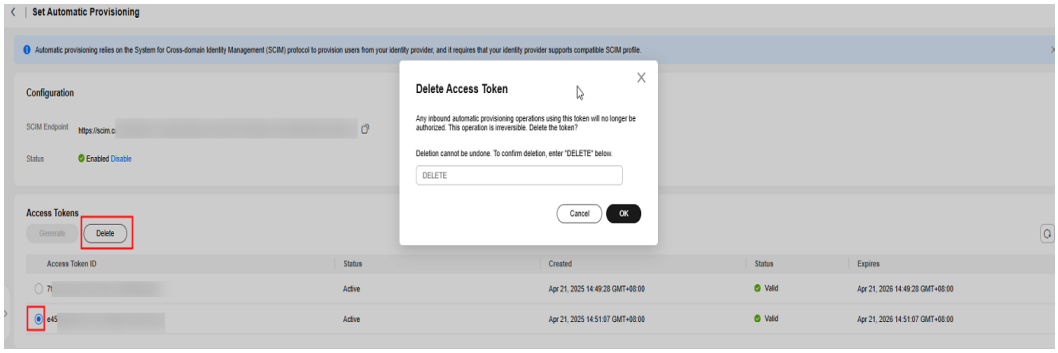
Figure 4-14 Generating an access token



Step 6 In the token list, select one or more tokens to be deleted and click **Delete**.

Step 7 In the displayed dialog box, enter **DELETE** and click **OK**.

Figure 4-15 Deleting an access token



NOTE

IAM Identity Center supports two access tokens at most. To generate additional access tokens, delete expired or unused access tokens.

----End

4.3.4 Enabling Manual Provisioning

Some IdPs do not have SCIM support or have an incompatible SCIM implementation. In this case, you can manually provision users and groups through the IAM Identity Center console. When you add users to IAM Identity Center, ensure that the username is the same as that in your IdP.

Procedure

After the identity source is changed to an external identity provider, the provisioning method is manual provisioning by default. If you want to change the provisioning method to manual provisioning, do as follows:

Step 1 Log in to the Huawei Cloud management console.

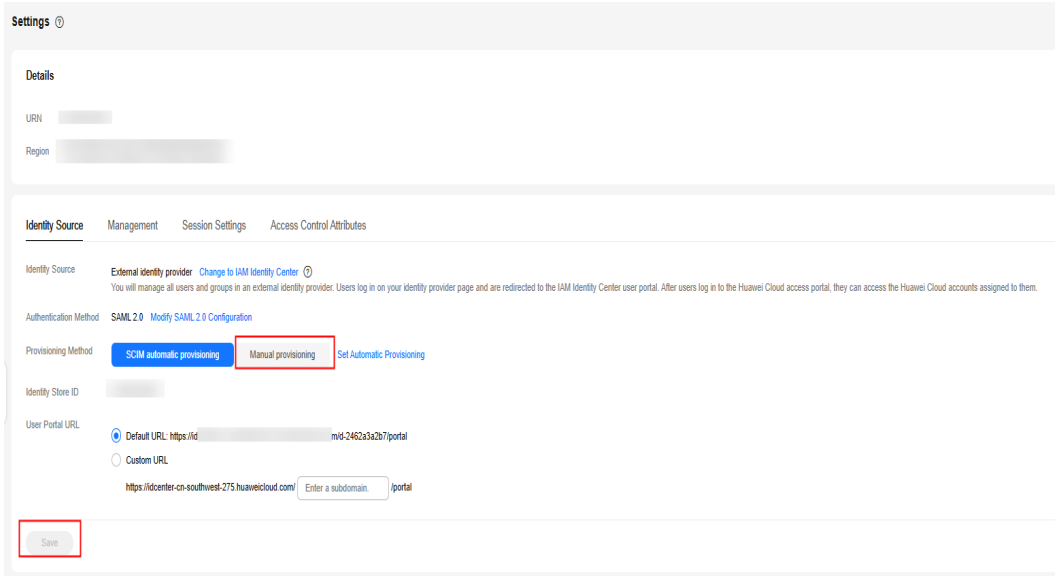
Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 On the **Identity Source** tab, select **Manual provisioning** for **Provisioning Method** and click **Save**.

After manual provisioning is enabled, create and manage users and groups in IAM Identity Center. For details, see **User Management** and **Group Management**.

Figure 4-16 Enabling manual provisioning



----End

4.3.5 Rotating Certificates

IAM Identity Center uses certificates to set up a SAML trust relationship between IAM Identity Center and your external identity provider. When you change the identity source to an external identity provider, you must also obtain at least one SAML 2.0 certificate from the external identity provider. SP certificates are usually generated manually when signed requests are required, while IdP certificates are usually included in the SAML metadata file and are automatically installed when you upload the IdP SAML metadata during identity source change.

You may need to import certificates periodically to rotate invalid or expired certificates issued by your identity provider. This helps prevent authentication disruption or downtime. The process of replacing old certificates with new ones is called certificate rotation. Certificates can be deleted only after you ensure that they are no longer in use by the associated identity provider.

You should also consider that some identity providers may not support multiple certificates. In this case, rotating a certificate may temporarily interrupt services for your users. After the certificate is rotated and the trust with the identity provider is re-established, services will be restored. You are advised to rotate certificates during off-peak hours.

NOTE

- If an existing SAML certificate is disclosed or handled improperly, you should immediately replace it and delete the old one.
- Each SP supports a maximum of two certificates, but only one certificate can be activated.
- The default validity period of an SP certificate is 10 years.
- All imported certificates are automatically activated. Currently, a maximum of two certificates are supported.

Rotating SP Certificates

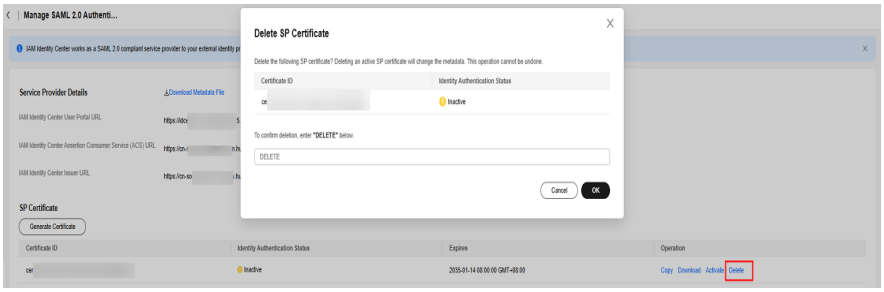
Step 1 Manually generate a certificate.

1. Log in to the Huawei Cloud management console.
2. Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.
3. Choose **Settings** in the navigation pane.
4. On the **Identity Source** tab, click **Modify SAML 2.0 Configuration** in the **Authentication Method** row.
5. On the displayed page, click **Generate Certificate**.
6. Locate the certificate and click **Activate** in the **Operation** column. The old certificate status automatically changes to inactive.

Step 2 Delete the old certificate.

1. On the **Manage SAML 2.0 Authentication** page, select the certificate to be deleted from the SP certificate list and click **Delete**.
2. In the displayed dialog box, enter **DELETE** and click **OK**.

Figure 4-17 Deleting a certificate



----End

Rotating IdP Certificates

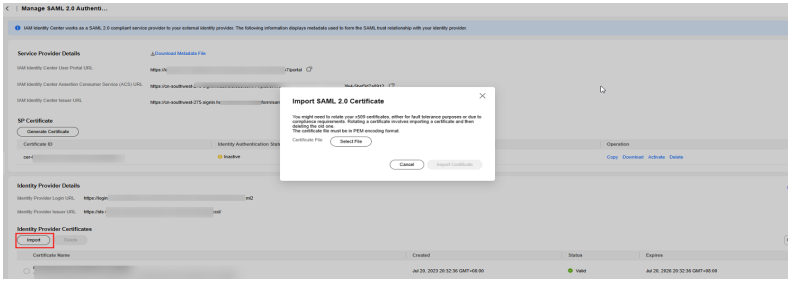
Step 1 Obtain a new certificate from your identity provider.

Go to the identity provider website and download the SAML 2.0 certificate. Make sure that the certificate file is downloaded in PEM encoding format. Most identity providers allow you to create multiple SAML 2.0 certificates, which are likely to be marked as disabled or inactive.

Step 2 Import the new certificate to IAM Identity Center.

1. Log in to the Huawei Cloud management console.
2. Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.
3. Choose **Settings** in the navigation pane.
4. On the **Identity Source** tab, click **Modify SAML 2.0 Configuration** in the **Authentication Method** row.
5. On the displayed page, click **Import**.
6. In the displayed dialog box, click **Select File**, select the obtained new certificate, and click **Import Certificate**.

Figure 4-18 Importing a certificate



Then IAM Identity Center will trust all incoming SAML messages signed from both of the certificates that you have imported.

Step 3 Activate the new certificate in the external identity provider.

Return to the identity provider website and mark the new certificate that you created earlier as primary or active. All SAML messages signed by the identity provider should be using the new certificate.

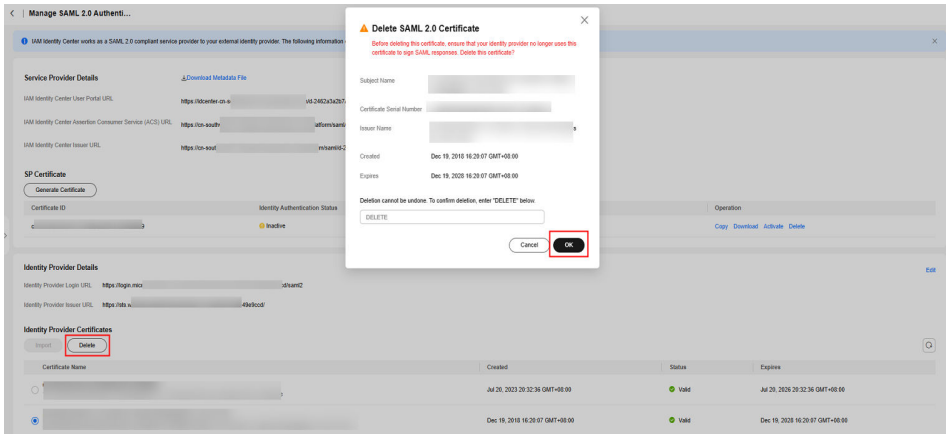
Step 4 Delete the old certificate.

NOTE

- Before deleting this certificate, ensure that your identity provider no longer uses this certificate to sign SAML responses.
- There must always be at least one valid certificate in the certificate list.

1. On the **Manage SAML 2.0 Authentication** page, select the certificates to be deleted in the IdP certificate list and click **Delete**.
2. In the displayed dialog box, enter **DELETE** and click **OK**.

Figure 4-19 Deleting a certificate



3. Return to the identity provider website and delete the old certificate.

----End

4.4 Supported Identity Providers

Microsoft Azure AD

IAM Identity Center supports automatic provisioning (synchronization) of user and group information from Microsoft Azure Active Directory (Azure AD) into IAM Identity Center using the SCIM v2.0 protocol. You configure this connection in Azure AD using the SCIM endpoint and access token that is created automatically by IAM Identity Center. When you configure SCIM synchronization, you create a mapping of your user attributes in Azure AD to the named attributes in IAM Identity Center. This causes the expected attributes to match between IAM Identity Center and your identity provider.

Okta

IAM Identity Center supports automatic provisioning (synchronization) of user and group information from Okta into IAM Identity Center using the SCIM v2.0 protocol. You configure this connection in Okta using the SCIM endpoint and access token that is created automatically by IAM Identity Center. When you configure SCIM synchronization, you create a mapping of your user attributes in Okta to the named attributes in IAM Identity Center. This causes the expected attributes to match between IAM Identity Center and your identity provider.

5 IAM Identity Center Resetting

If you no longer need to use IAM Identity Center, intend to enable IAM Identity Center in a different region, or intend to create a new configuration from scratch, you can delete all data configured in IAM Identity Center.

IAM Identity Center is a project-level service. If you have enabled IAM Identity Center in a region and want to use it in another region, you need to delete the configuration in the original region before enabling IAM Identity Center in another region.

Procedure

Step 1 Log in to the Huawei Cloud management console.

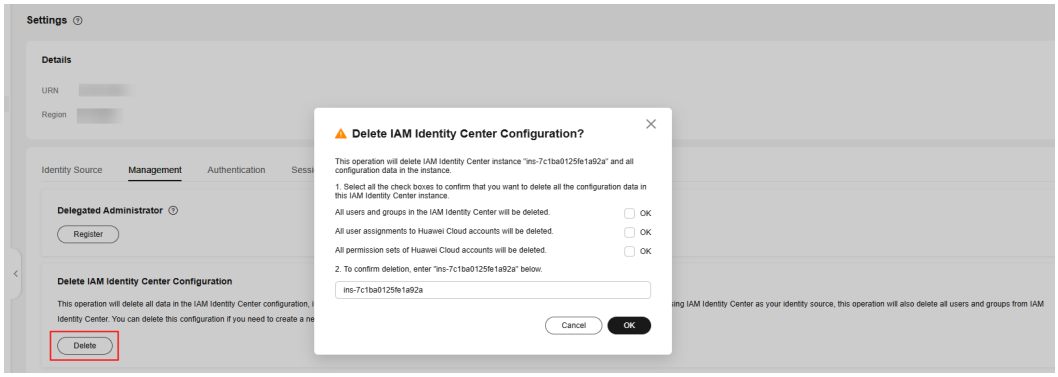
Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 On the **Management** tab, click **Delete**.

Step 5 In the displayed dialog box, select each checkbox to acknowledge the deletion, enter the IAM Identity Center instance ID in the text box, and click **OK**.

Figure 5-1 Deleting the IAM Identity Center configuration



NOTE

When the IAM Identity Center configuration is deleted, all the data in that configuration is deleted and cannot be recovered.

----End

6 MFA Management

6.1 MFA Overview

What Is Multi-Factor Authentication (MFA)?

Multi-factor authentication (MFA) is a popular method that adds an additional layer of authentication on top of the username and password. If you enable MFA authentication, users need to enter the username and password as well as a verification code before they can log in to the console.

To improve security, you are advised to enable MFA in IAM Identity Center.

Supported MFA Devices

IAM Identity Center supports the following MFA devices:

- Authenticator App

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

- Security key and built-in authenticator

  FIDO2 is a standard based on public key cryptography. It includes CTAP2 and WebAuthn. FIDO credentials are phishing-resistant because they are unique to specific websites.

  A security key is a FIDO2-compatible external hardware authenticator that you can purchase and connect to your device via USB, BLE, or NFC. When you are prompted for MFA, you only need to touch a hardware security key such as YubiKey to verify your identity. The most common security keys (including YubiKey) can create device-bound FIDO credentials.

  A built-in authenticator is pre-installed on a computer or mobile phone that uses biometric data. Typical built-in authenticators include Apple Touch ID and Windows Hello. If your device has a built-in authenticator that is compatible with FIDO2, you can use a fingerprint, face, or device PIN as a second factor.

6.2 MFA Authentication

6.2.1 Enabling MFA

You can enable MFA on the IAM Identity Center console for improved security.

NOTE

If you are using an external identity provider as the identity source, you will need to configure MFA in that external identity provider. If you are using IAM Identity Center as the identity source, you can configure MFA in IAM Identity Center as follows.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 Click the **Authentication** tab.

Step 5 In **Prompt Users for MFA**, determine whether to prompt users for MFA based on the level of security that your service needs.

- **Only when their sign-in context changes (context-aware)**

  IAM Identity Center provides users the option to trust their device during login. After a user selects this option, IAM Identity Center prompts the user for MFA once and analyzes the login context (such as device, browser, and IP address) for the user's subsequent logins. IAM Identity Center determines if the user is logging in with a previously trusted context. If the user's login context changes, IAM Identity Center prompts the user for MFA in addition to their username and password.

  This mode provides ease of use for users who frequently log in from their workplace, so they do not need to complete MFA on every login. They are only prompted for MFA if their login context changes.

  NOTE

  The validity period of the device trust is seven days. After seven days, you will need to perform MFA authentication again.

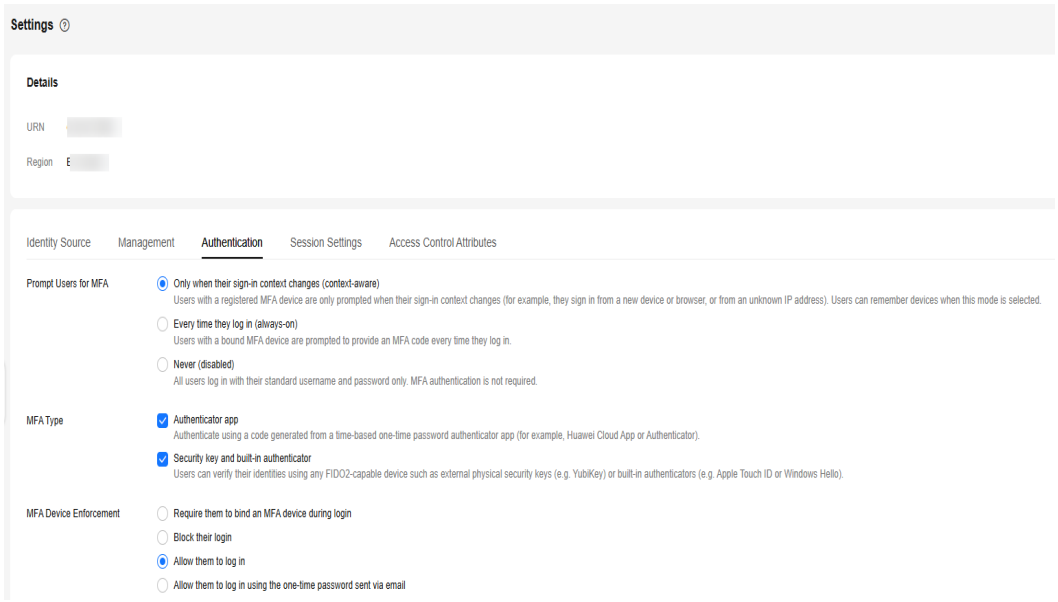
- **Every time they log in (always-on)**

  IAM Identity Center requires that users with a bound MFA device will be prompted to provide an MFA code every time they log in. You should use this mode if you have organizational or compliance policies that require your users to complete MFA every time they log in to the user portal.

- **Never (disabled)**

  MFA authentication is disabled. All users will log in with their standard username and password only.

Figure 6-1 Enabling MFA



Step 6 Click **Save**.

----End

6.2.2 Selecting an MFA Type

You can select a device type for MFA authentication when IAM Identity Center users are prompted for MFA.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

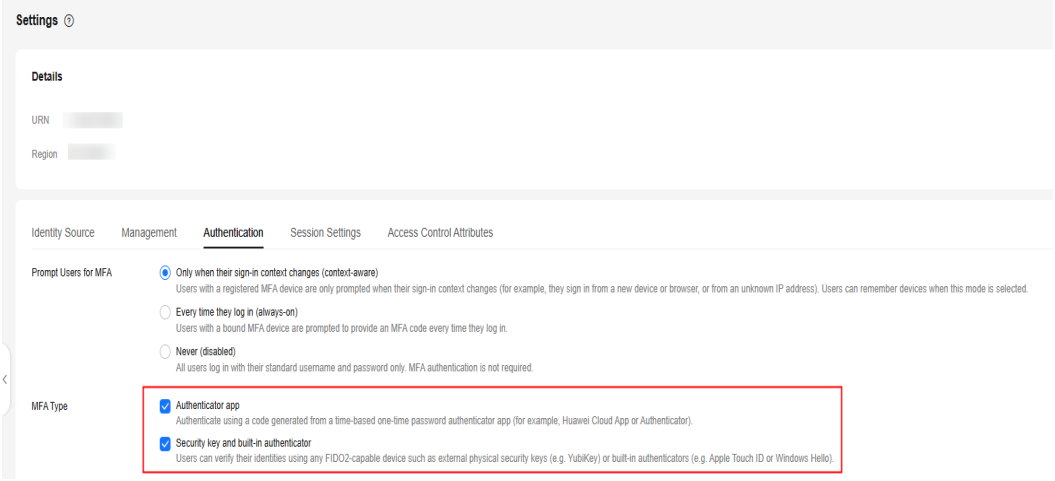
Step 3 Choose **Settings** in the navigation pane.

Step 4 Click the **Authentication** tab.

Step 5 In **MFA Type**, select one of the following MFA types based on service requirements. You can select two MFA types at the same time. For details, see **Supported MFA Devices**.

- Authenticator app
- Security key and built-in authenticator

Figure 6-2 Selecting an MFA type



Step 6 Click **Save**.

----End

6.2.3 Configuring MFA Device Enforcement

You can determine whether IAM Identity Center users must have a registered MFA device when they log in to the user portal.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 Click the **Authentication** tab.

Step 5 In **MFA Device Enforcement**, select one of the following options based on service requirements:

- **Require them to bind an MFA device during login**

  Use this option when you want to require users who do not yet have a bound MFA device, to bind a device by themselves during login following a successful password authentication. For details, see **Binding an MFA Device**.

- **Block their login**

  Use this option when you want to enforce MFA authentication for every login.

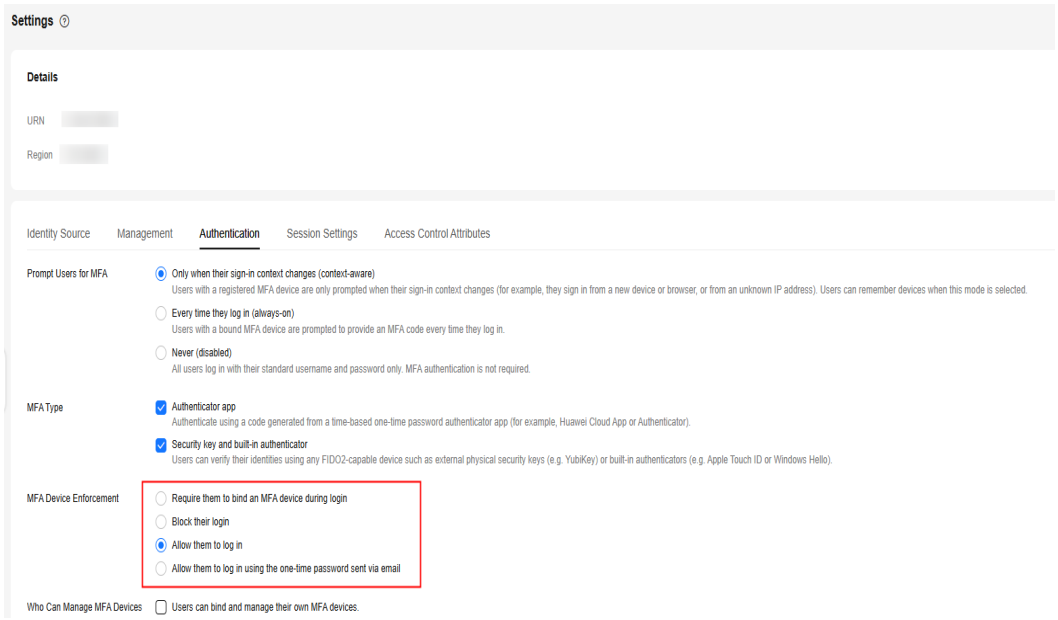
- **Allow them to log in**

  Use this option when you do not require MFA authentication for user logins.

- **Allow them to log in using the one-time password sent via email**

  Use this option when you want to send a verification code to a user by email.

Figure 6-3 Configuring MFA device enforcement



Step 6 Click **Save**.

----End

6.2.4 Allowing Users to Bind Their Own MFA Devices

You can enable users to bind their own MFA devices.

Procedure

Step 1 Log in to the Huawei Cloud management console.

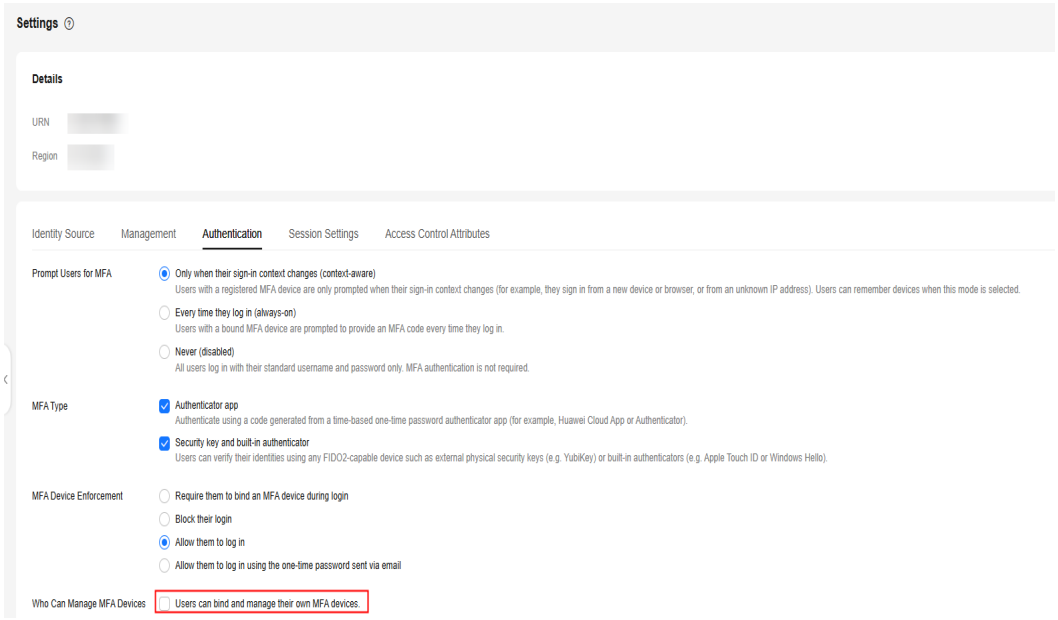
Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 Choose **Settings** in the navigation pane.

Step 4 Click the **Authentication** tab.

Step 5 In **Who Can Manage MFA Devices**, select **Users can bind and manage their own MFA devices.**

Figure 6-4 Allowing users to bind their own MFA devices



Step 6 Click **Save**.

----End

6.3 MFA Configuration

6.3.1 Binding an MFA Device

You must have physical access to the user's MFA device so that you can add it. For example, you might configure MFA for a user who will use an MFA device running on a smartphone. In this case, you must have the smartphone available in order to finish the wizard. For this reason, you might want to let users configure and manage their own MFA devices. For details, see **Allowing Users to Bind Their Own MFA Devices**.

Binding an MFA Device

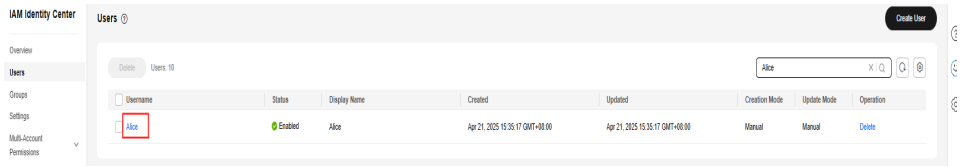
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Users**.

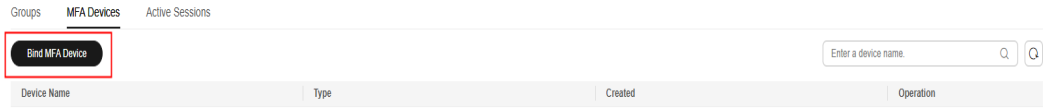
Step 4 In the user list, click a username to go to the user details page.

Figure 6-5 Selecting a user



Step 5 On the **MFA Devices** tab, and click **Bind MFA Device**.

Figure 6-6 Binding an MFA device



Step 6 On the displayed page, select one of the following MFA device types and perform operations as instructed:

- Authenticator app

  On the **Bind Virtual MFA Device** page, the configuration information, including the QR code, of the new MFA device is displayed. Follow the prompts to bind a virtual MFA device.

  a. Install a compatible virtual MFA device (authenticator app) on your mobile phone.

  b. Bind the virtual MFA device by scanning the QR code or manually entering the secret key.

  - Scan the QR code

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

  - 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 phone.

  c. View the dynamic code of the virtual MFA deviceon the MFA application. The code is automatically updated every 30 seconds.

  d. In the **Bind Virtual MFA Device** dialog box, enter the dynamic code.

  e. Click **OK**.

- Security key

  In the **Add Security Key** dialog box, follow the instructions displayed on the browser or platform.

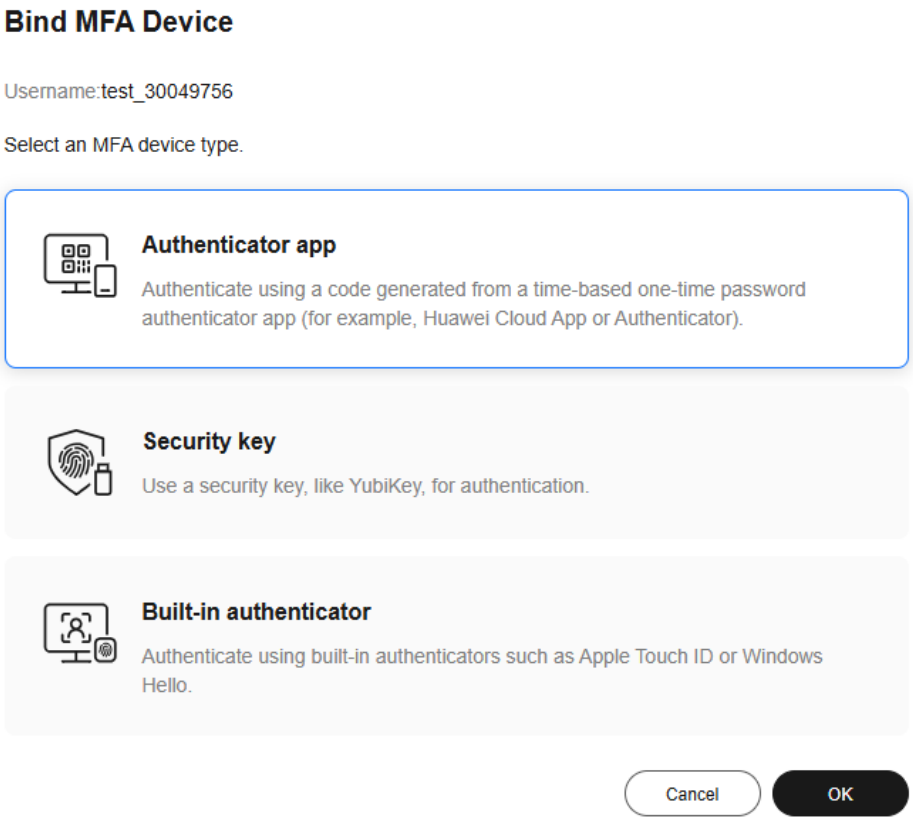
  NOTE

  - The experience may vary in different operating systems and browsers, so follow the instructions displayed by your browser or platform.
  - If you bind all of the MFA device types, the security key and built-in authenticator take precedence over the authenticator app when users log in to the user portal.

- Built-in authenticator

  Use your fingerprint, face, or PIN code to authenticate your identity following the instructions displayed on the browser or platform.

Figure 6-7 Binding an MFA device



Step 7 View the bound MFA device in the list.

----End

6.3.2 Managing a User's MFA Device

You can rename or delete a user's MFA device.

Renaming an MFA Device

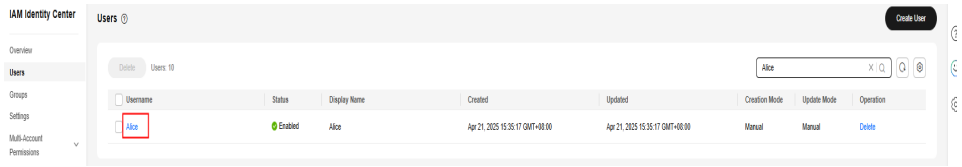
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Users**.

Step 4 In the user list, click a username to go to the user details page.

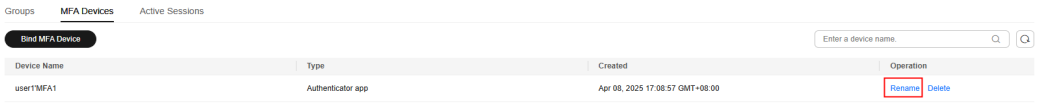
Figure 6-8 Selecting a user



Step 5 On the **MFA Devices** tab, locate the target MFA device and click **Rename** in the **Operation** column.

Step 6 Enter a new MFA device name and click **OK**.

Figure 6-9 Renaming an MFA device



----End

Deleting an MFA Device

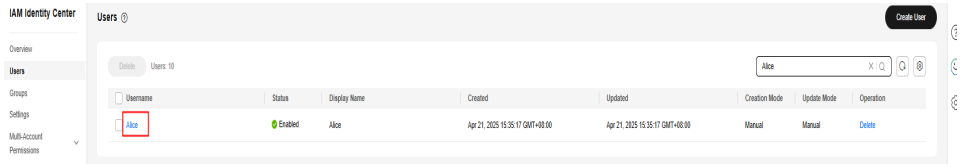
Step 1 Log in to the Huawei Cloud management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.

Step 3 In the navigation pane, choose **Users**.

Step 4 In the user list, click a username to go to the user details page.

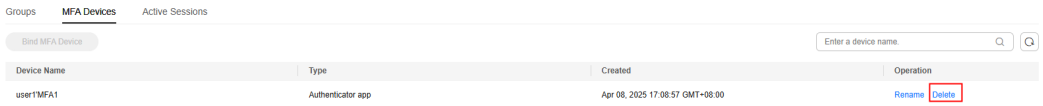
Figure 6-10 Selecting a user



Step 5 On the **MFA Devices** tab, locate the target MFA device and click **Delete** in the **Operation** column.

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

Figure 6-11 Deleting an MFA device



----End

7 Using IAM to Grant Access to IAM Identity Center

7.1 Creating a User and Granting IAM Identity Center Permissions

You can use **Identity and Access Management (IAM)** for fine-grained permissions control for your IAM Identity Center. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing IAM Identity Center resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or a cloud service to perform efficient O&M on your IAM Identity Center resources.

If your account does not require individual IAM users, you may skip over this section.

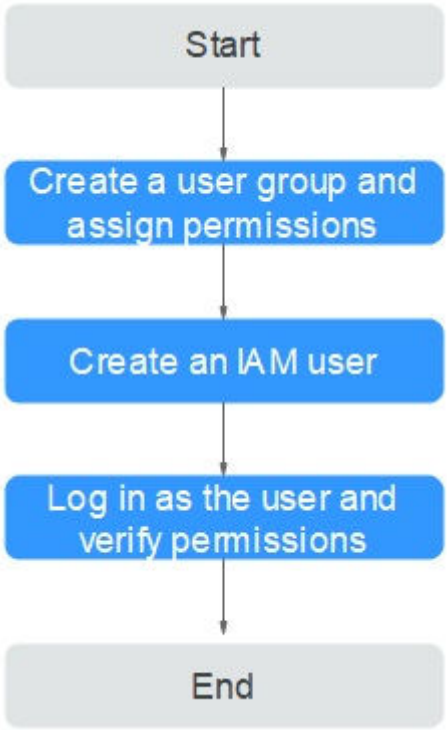
This section describes the procedure for granting permissions (see **Figure 7-1**).

Prerequisites

Before granting permissions to user groups, learn about system-defined permissions in for IAM Identity Center. To grant permissions for other services, learn about all **system-defined permissions**.

Process Flow

Figure 7-1 Process of granting IAM Identity Center permissions



1. On the IAM console, **create a user group and grant it permissions** (**IdentityCenter ReadOnlyAccess** as an example).
2. **Create an IAM user and add it to the created user group**.
3. **Log in as the created IAM user** and verify the **IdentityCenter ReadOnlyAccess** permission.

7.2 Creating IAM Custom Policies for IAM Identity Center

You can create custom policies to supplement the system-defined policies of IAM Identity Center.

To create a custom policy, choose either visual editor or JSON.

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

For details, see **Creating a Custom Policy**. The following lists examples of common IAM Identity Center custom policies.

Example Custom Policies

- Example 1: Grant permission to create a permission set.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "IdentityCenter:permissionSet:create"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "organizations:delegatedAdministrators:list"
         ]
      }
   ]
}
```

- Example 2: Grant permission to deny permission set deletion.

  A policy with only "Deny" permissions must be used together with other policies. If the permissions granted to an IAM user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  Assume that you want to grant the permissions of the **IdentityCenter FullAccess** policy to a user but want to prevent them from deleting permission sets. You can create a custom policy for denying permission set deletion, and attach this policy together with the **IdentityCenter FullAccess** policy to the user. As an explicit deny in any policy overrides any allows, the user can perform all operations in IAM Identity Center excepting deleting permission sets.

  Example policy denying permission set deletion:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "IdentityCenter:permissionSet:delete"
         ]
      }
   ]
}
```

- Example 3: Create a custom policy containing multiple actions.

  A custom policy can contain the actions of one or multiple services that are of the same type (global or project-level).

  Example policy containing multiple actions:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "IdentityCenter:permissionSet:delete",
            "IdentityCenter:user:create",
            "IdentityCenter:permissionSet:create"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
```



```
            "organizations:delegatedAdministrators:list"
        ]
    }
  ]
}
```


8 Using CTS to Audit IAM Identity Center Operations

8.1 Key Operations Supported by CTS

With Cloud Trace Service (CTS), you can record IAM Identity Center operations for later query, auditing, and backtracking.

Table 8-1 IAM Identity Center operations that can be recorded by CTS

Operation	Resource Type	Event Name
Enabling IAM Identity Center	Instance	StartIdentityCenter
Disabling IAM Identity Center	Instance	DeleteIdentityCenter
Registering a region	Instance	RegisterRegion
Updating single sign-on (SSO) configuration	Instance	UpdateSsoConfiguration
Updating the MFA device management in the identity store	Instance	UpdateMfaDeviceManagementForIdentityStore
Adding a user-defined domain name	Instance	CreateAlias
Enabling access control attributes for a specified instance	Instance	CreateInstanceAccessControlAttributeConfiguration
Disabling access control attributes for a specified instance	Instance	DeleteInstanceAccessControlAttributeConfiguration

Operation	Resource Type	Event Name
Updating access control attributes for a specified instance	Instance	UpdateInstanceAccess-ControlAttributeConfigu-ration
Assigning users/groups to a specified account with a specified permission set	AccountAssignment	CreateAccountAssign-ment
Removing users/groups from a specified account with a specified permission set	AccountAssignment	DeleteAccountAssign-ment
Deleting all permission sets associated with a user/group	AccountAssignment	DisassociateProfile
Creating a permission set in a specified IAM Identity Center instance	PermissionSet	CreatePermissionSet
Deleting a specified permission set	PermissionSet	DeletePermissionSet
Updating a specified permission set	PermissionSet	UpdatePermissionSet
Attaching a system-defined policy to a permission set	PermissionSet	AttachManagedPolicyTo-PermissionSet
Detaching a system-defined policy from a permission set	PermissionSet	DetachManagedPolicy-FromPermissionSet
Attaching a system-defined role to a permission set	PermissionSet	AttachManagedRoleTo-PermissionSet
Detaching a system-defined role from a permission set	PermissionSet	DetachManagedRole-FromPermissionSet
Attaching a specified permission set to a specified account	PermissionSet	ProvisionPermissionSet
Deleting a custom policy from a specified permission set	PermissionSet	DeleteCustomPolicy

Operation	Resource Type	Event Name
Attaching a custom policy to a permission set	PermissionSet	PutCustomPolicy
Generating a credential for an IAM Identity Center user after user login	User	Authenticate
Activating a device authorization code	User	ActiveDevice
Canceling a device authorization code	User	CancelDevice
Creating a user	User	CreateUser
Deleting a user	User	DeleteUser
Updating a user	User	UpdateUser
Disabling a user	User	DisableUser
Enabling a user	User	EnableUser
Creating a virtual MFA device	User	CreateMfaDeviceForUser
Deleting a virtual MFA device	User	DeleteMfaDeviceForUser
Updating MFA information	User	UpdateMfaDeviceForUser
Sending an email containing the password reset link or a one-time password	User	UpdatePwdMode
Resetting a user password	User	ResetPassword
Sending an email verification link	User	VerifyEmail
Updating the email verification status	User	UpdateEmailStatus
Creating a group	Group	CreateGroup
Deleting a group	Group	DeleteGroup
Updating a group	Group	UpdateGroup
Adding a user to a group	GroupMembership	CreateGroupMembership

Operation	Resource Type	Event Name
Removing a user from a group	GroupMembership	DeleteGroupMembership
Batch adding IAM Identity Center users to groups	GroupMembership	BatchCreateMembership
Batch removing IAM Identity Center users from groups	GroupMembership	BatchDeleteMembership
Batch replacing IAM Identity Center users in groups	GroupMembership	BatchReplaceMembership
Creating external identity provider configuration	IDP	CreateExternalIdpConfigurationForDirectory
Enabling external identity provider	IDP	EnableExternalIdpConfigurationForDirectory
Deleting external identity provider configuration	IDP	DeleteExternalIdpConfigurationForDirectory
Disabling external identity provider	IDP	DisableExternalIdpConfigurationForDirectory
Updating external identity provider configuration	IDP	UpdateExternalIdpConfigurationForDirectory
Deleting a certificate	IDP	DeleteExternalIdpCertificate
Importing a certificate	IDP	ImportExternalIdpCertificate
Creating a bearer token	IDP	CreateBearerToken
Creating the tenant information corresponding to the identity source	IDP	CreateProvisioningTenant
Deleting a bearer token	IDP	DeleteBearerToken
Deleting the tenant information corresponding to the identity source	IDP	DeleteProvisioningTenant
Adding tags to the specified resource	Tag	CreateTagResource

Operation	Resource Type	Event Name
Deleting specified tags from specified resources	Tag	DeleteTagResource

8.2 Viewing CTS Traces in the Trace List

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in Object Storage Service (OBS) buckets. Cloud Trace Service (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

- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, you must 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 one minute later and query data traces five minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.
- 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.
- 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 **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

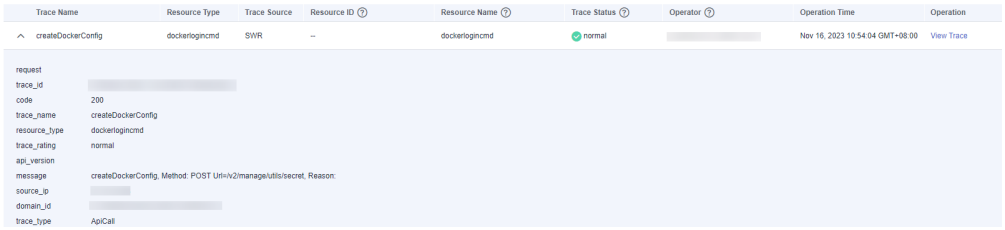
Viewing Real-Time Traces in the Trace List of the Old Edition

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 **Go to 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.

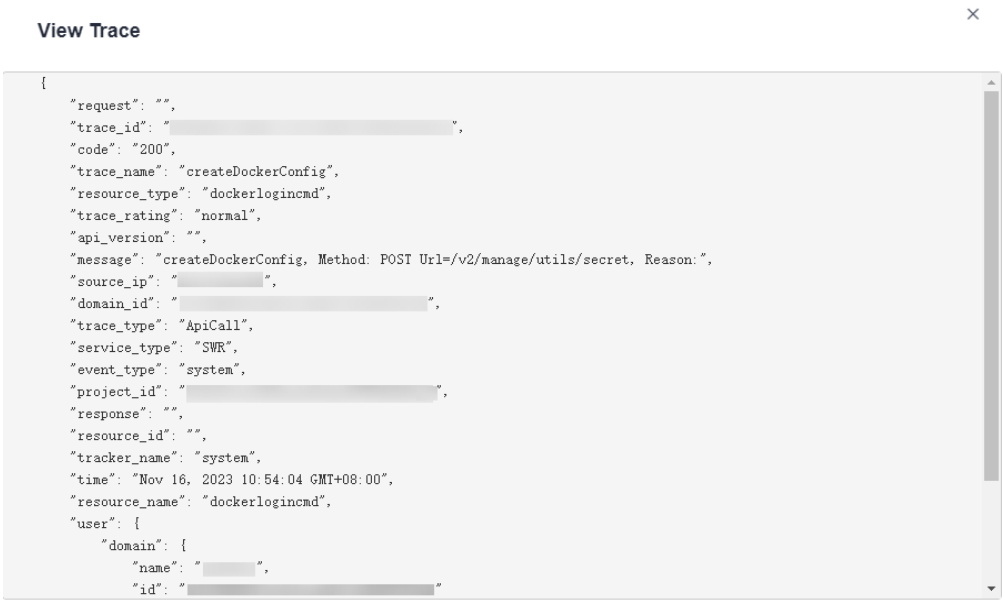
- If you select **Trace name** for **Search By**, specify a trace name.
- If you select **Resource name** for **Search By**, specify a resource name.

– **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.

9 Quotas

What Is a Quota?

A quota is a limit on the quantity or capacity of a certain type of service resources available to you, for example, the maximum number of IAM Identity Center users or groups that you can create.

If the current resource quota cannot meet your service requirements, you can apply for a higher quota.

