IAM Identity Center

Getting Started

Issue	01
Date	2023-08-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Notice

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

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

Contents

1 Overview....1

2 Making Preparations.... 3

3 Creating Users and Permission Sets....5

4 Associating Accounts with Users and Permission Sets....12

5 Logging In as an IAM Identity Center User and Accessing Resources....15

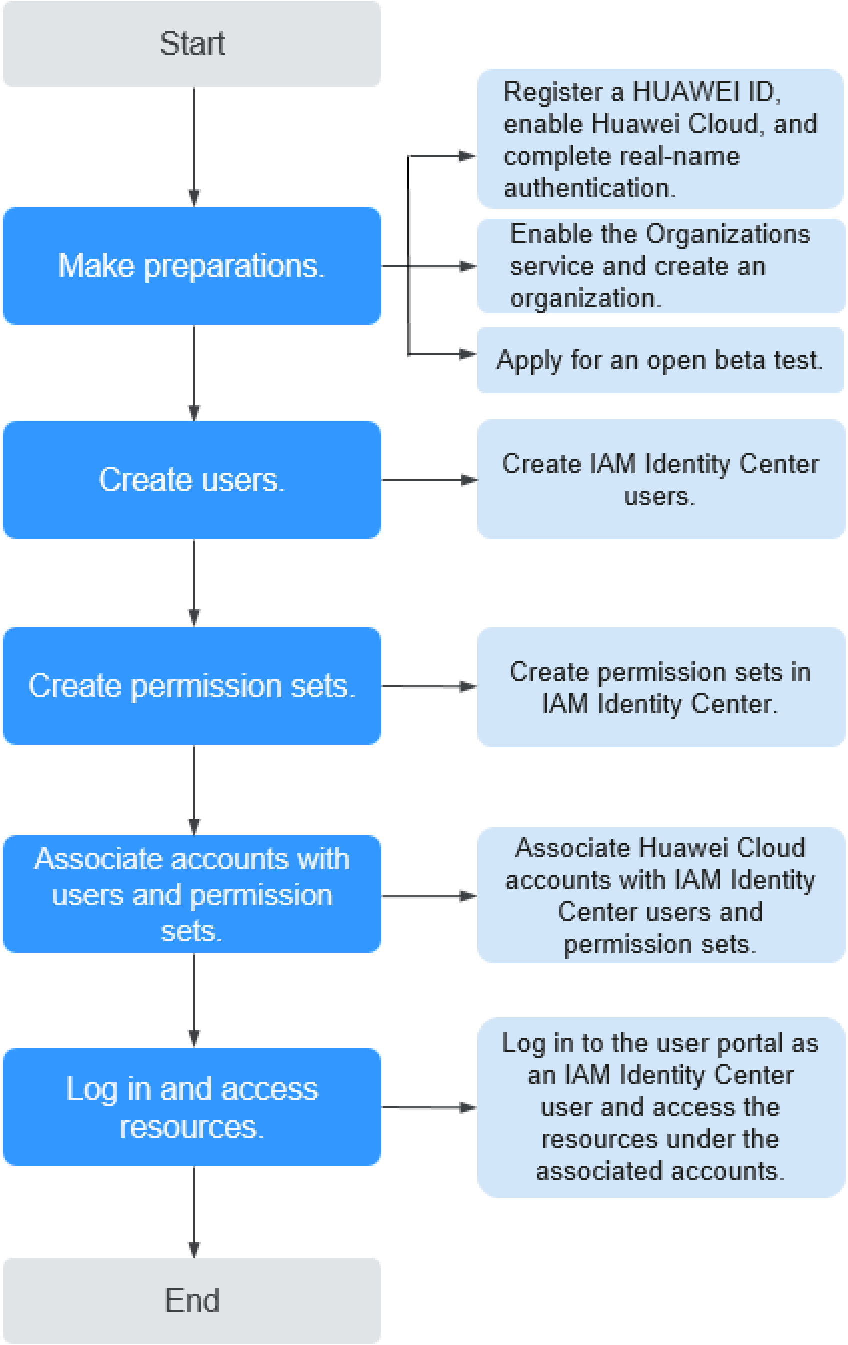
6 Change History.... 17

1 Overview

Read this chapter if you are using IAM Identity Center for the first time. It helps you quickly familiarize yourself with the main functions of IAM Identity Center.

The following figure shows how to use IAM Identity Center.

Figure 1-1 Flowchart


Start
Make preparations.
Register a HUAWEI ID, enable Huawei Cloud, and complete real-name authentication.
Enable the Organizations service and create an organization.
Apply for an open beta test.
Create users.
Create IAM Identity Center users.
Create permission sets.
Create permission sets in IAM Identity Center.
Associate accounts with users and permission sets.
Associate Huawei Cloud accounts with IAM Identity Center users and permission sets.
Log in and access resources.
Log in to the user portal as an IAM Identity Center user and access the resources under the associated accounts.
End

2 Making Preparations

Before using IAM Identity Center, you need to prepare as described in the following sections:

- **Registering a HUAWEI ID, Enabling Huawei Cloud, and Completing Real-Name Authentication**
- **Enabling the Organizations Service and Creating an Organization**
- **Applying for an Open Beta Test and Enabling IAM Identity Center**

Registering a HUAWEI ID, Enabling Huawei Cloud, and Completing Real-Name Authentication

If you already have a Huawei Cloud account, skip this part. If you do not have a Huawei Cloud account:

1. Log in to the **Huawei Cloud official website**, and click **Register** in the upper right corner.
2. Register a HUAWEI ID as prompted.
3. Read and agree to the terms, and click **Enable**.

   For details, see **Registering a HUAWEI ID and Enabling Huawei Cloud Services**.
4. Complete real-name authentication by following the instructions in **Real-Name Authentication Overview**.

NOTE

IAM Identity Center is a free service. You do not need to top up your account.

Enabling the Organizations Service and Creating an Organization

IAM Identity Center obtains member account information from organizations defined in the Organizations service. Before using IAM Identity Center, you must enable the Organizations service and create an organization. Then, you can log in to IAM Identity Center using the organization's management account.

Before using the Organizations service, you need to enable the **Enterprise Center** function. You must use the master account of Enterprise Center to create an organization.

Step 1 Go to the Enterprise Center console.

Step 2 Click **Enable for Free**.

The **Enable Enterprise Center** dialog box is displayed.

Step 3 Select **I have read and agree to the HUAWEI CLOUD Enterprise Management Service Agreement** and click **Enable for Free**. Your account will become an enterprise master account. For details, see **Enabling Enterprise Center**.

Step 4 Go to the Organizations console.

Step 5 Click **Enable Organizations** to enable the Organizations service.

Step 6 After the Organizations service is enabled, your organization and the root are automatically created, and your login account is defined as the management account. For details, see **Creating an Organization**.

Step 7 Invite an account to join your organization. For details, see **Inviting an Account to Join Your Organization**.

----End

Applying for an Open Beta Test and Enabling IAM Identity Center

IAM Identity Center is now under open beta test. Before using IAM Identity Center, you need to apply for an open beta test. Enterprise users can apply for a free trial.

1. Log in to the **Huawei Cloud console**.
2. Click ☰ in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.
3. Click **Apply Now** to switch to the page for applying for open beta test qualification.
4. Provide required information, including your enterprise size, proportion of R&D engineers, application scenario, current business stage, and business details.
5. Select the **Agree OBT Trial Service Agreement** check box to confirm that you have read and agree to the terms and conditions in the agreement, and click **Apply For The Beta**.

   The review result will be sent to you via email and SMS message within five working days.
6. Choose **Resources** > **Open Beta Tests** in the menu bar to view your application status.
7. After your application is approved, click **Enable Now** on the **IAM Identity Center** page to enable the service.

   After IAM Identity Center is enabled, the system automatically creates a service instance and an identity source, and generates a user portal URL.

3 Creating Users and Permission Sets

Creating Users

After IAM Identity Center is enabled, you need to create Identity Center users.

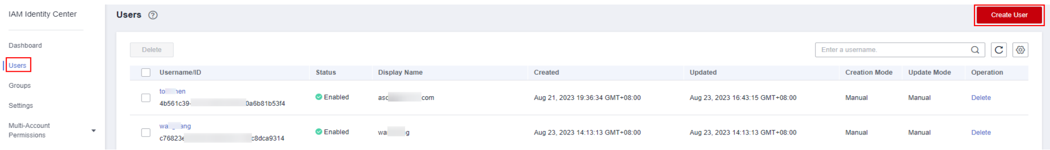
Step 1 Log in to the **Huawei Cloud console**.

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.

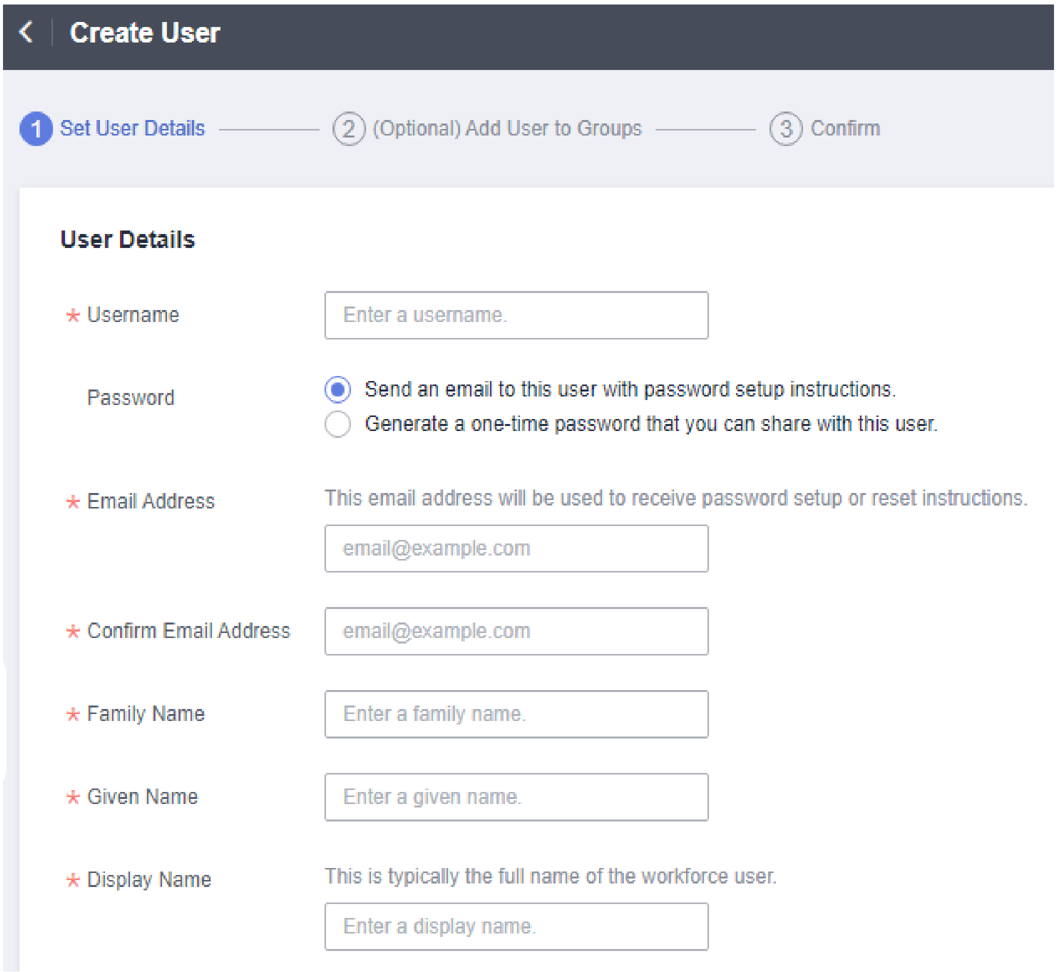
Figure 3-1 Creating users



□	Username/ID	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
□	to[redacted]en 4b561c39-[redacted]0a6b81b53f4	Enabled	asc[redacted]com	Aug 21, 2023 19:36:34 GMT+08:00	Aug 23, 2023 16:43:15 GMT+08:00	Manual	Manual	Delete
□	wa[redacted]ang c76823[redacted]c8dca9314	Enabled	wa[redacted]g	Aug 23, 2023 14:13:13 GMT+08:00	Aug 23, 2023 14:13:13 GMT+08:00	Manual	Manual	Delete

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

Figure 3-2 Configuring basic information



Create User

1 Set User Details — 2 (Optional) Add User to Groups — 3 Confirm

User Details

* Username: Enter a username.

Password:
● Send an email to this user with password setup instructions.
○ Generate a one-time password that you can share with this user.

* Email Address: This email address will be used to receive password setup or reset instructions.
email@example.com

* Confirm Email Address: email@example.com

* Family Name: Enter a family name.

* Given Name: Enter a given name.

* Display Name: This is typically the full name of the workforce user.
Enter a display name.

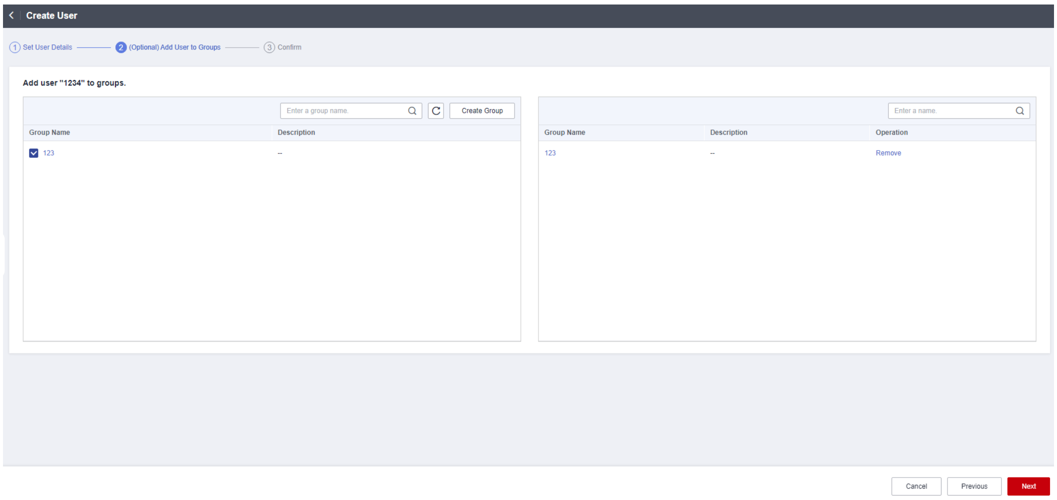
Table 3-1 Basic parameters

Parameter	Description
Username	IAM Identity Center username, which uniquely identifies a user. 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.

Parameter	Description
Email Address	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.
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 3-3 (Optional) Adding a user to groups



Add user "1234" to groups.

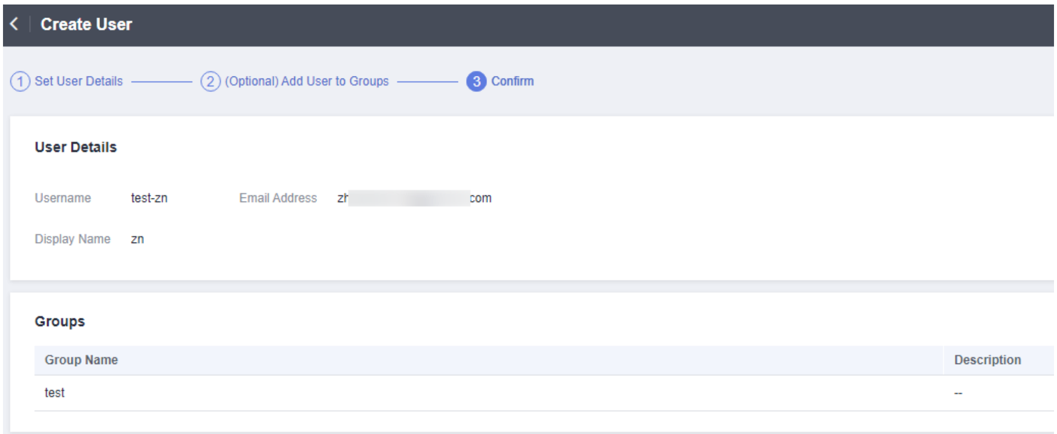
Group Name	Description
☑ 123	--

Group Name	Description	Operation
123	--	Remove

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 3-4 Confirming user creation



User Details

Username test-zn
Email Address zh[redacted]com
Display Name zn

Groups

Group Name	Description
test	--

----End

Creating Permission Sets

A permission set defines a collection of one or more IAM policies and controls the permissions of IAM Identity Center users to access resources. 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.

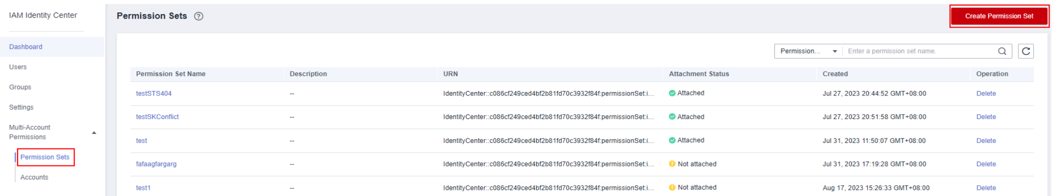
Step 1 Log in to the **Huawei Cloud console**.

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.

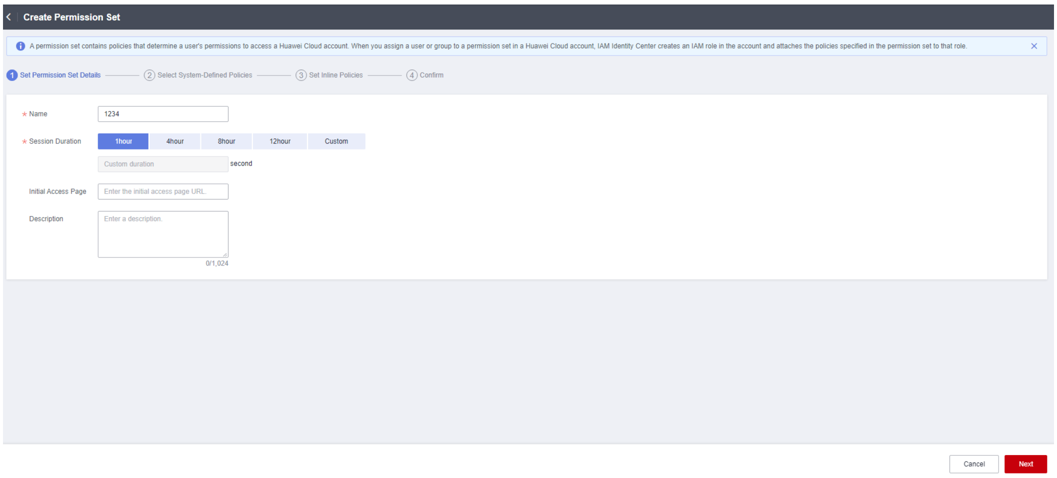
Figure 3-5 Creating a permission set



Permission Set Name	Description	URN	Attachment Status	Created	Operation
testSTS404	--	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84f:permissionSet:i...	Attached	Jul 27, 2023 20:44:52 GMT+08:00	Delete
testSKConflict	--	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84f:permissionSet:i...	Attached	Jul 27, 2023 20:51:58 GMT+08:00	Delete
test	--	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84f:permissionSet:i...	Attached	Jul 31, 2023 11:50:07 GMT+08:00	Delete
fafaagfargarg	--	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84f:permissionSet:i...	Not attached	Jul 31, 2023 17:19:28 GMT+08:00	Delete
test1	--	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84f:permissionSet:i...	Not attached	Aug 17, 2023 15:26:33 GMT+08:00	Delete

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

Figure 3-6 Setting permission set details



A permission set contains policies that determine a user's permissions to access a Huawei Cloud account. When you assign a user or group to a permission set in a Huawei Cloud account, IAM Identity Center creates an IAM role in the account and attaches the policies specified in the permission set to that role.

* Name: 1234

* Session Duration: 1hour

Custom duration second

Initial Access Page: Enter the initial access page URL.

Description: Enter a description.

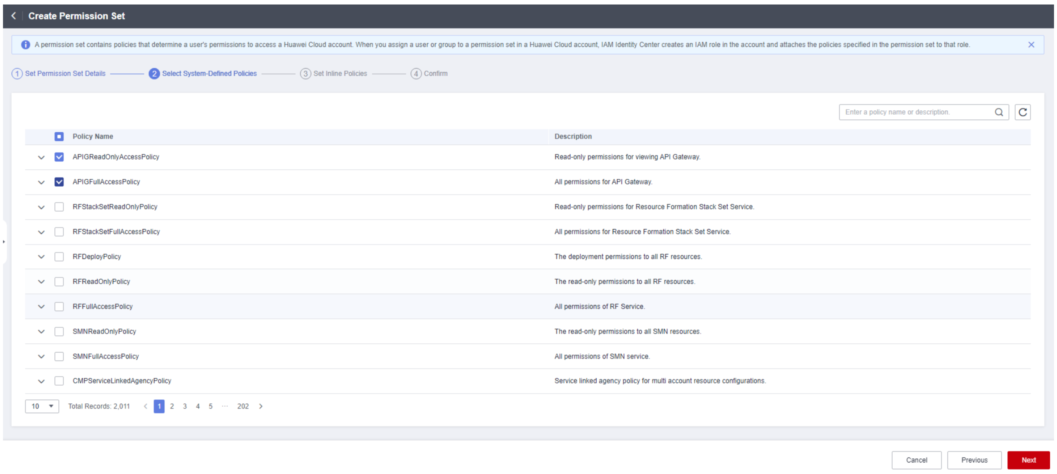
0/1,024

Table 3-2 Permission set details

Parameter	Description
Name	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.
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	Remarks for the permission set. The value is user-defined.

Step 6 In the **Select System-Defined Policies** step, select system-defined policies that you want to use for the permission set and click **Next**.

Figure 3-7 Selecting system-defined policies



Create Permission Set

A permission set contains policies that determine a user's permissions to access a Huawei Cloud account. When you assign a user or group to a permission set in a Huawei Cloud account, IAM Identity Center creates an IAM role in the account and attaches the policies specified in the permission set to that role.

① Set Permission Set Details — ② Select System-Defined Policies — ③ Set Inline Policies — ④ Confirm

Enter a policy name or description.

	Policy Name	Description
☑	APIGReadOnlyAccessPolicy	Read-only permissions for viewing API Gateway.
☑	APIGFullAccessPolicy	All permissions for API Gateway.
□	RFStackSetReadOnlyPolicy	Read-only permissions for Resource Formation Stack Set Service.
□	RFStackSetFullAccessPolicy	All permissions for Resource Formation Stack Set Service.
□	RFDeployPolicy	The deployment permissions to all RF resources.
□	RFReadOnlyPolicy	The read-only permissions to all RF resources.
□	RFFullAccessPolicy	All permissions of RF Service.
□	SMNReadOnlyPolicy	The read-only permissions to all SMN resources.
□	SMNFullAccessPolicy	All permissions of SMN service.
□	CMPServiceLinkedAgencyPolicy	Service linked agency policy for multi account resource configurations.

10 Total Records: 2,011 ‹ 1 2 3 4 5 ··· 202 ›

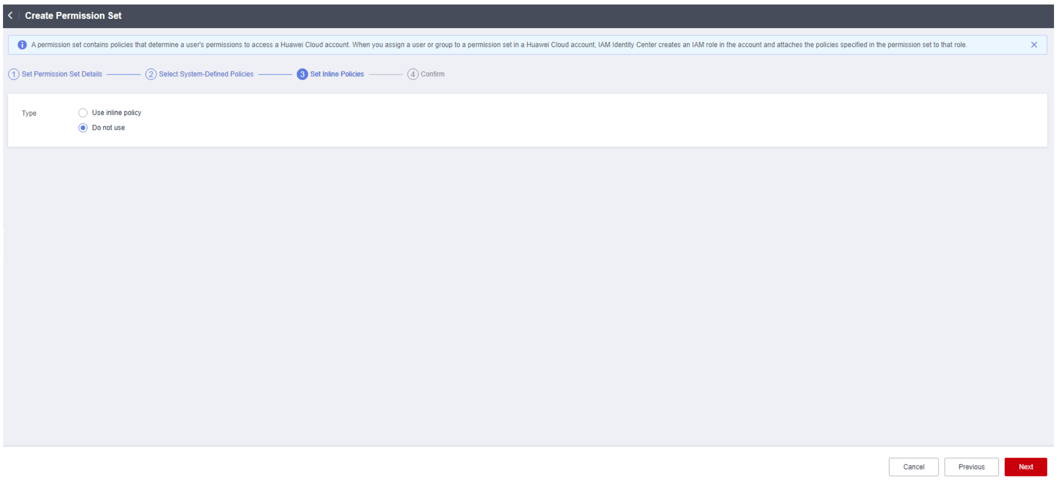
Step 7 On the **Set Inline Policies** tab, select whether to use an inline policy and click **Next**.

- **Use inline policy**: If the system-defined policies cannot meet your requirements, you can select this option and edit the JSON document in the text box below.

  The system automatically verifies the syntax. If "Syntax error in the inline policy." is displayed, modify the JSON statement according to **Policy Syntax**.

- **Do not use**: If the system-defined policies can meet your requirements, select this option.

Figure 3-8 Set inline policies



Create Permission Set

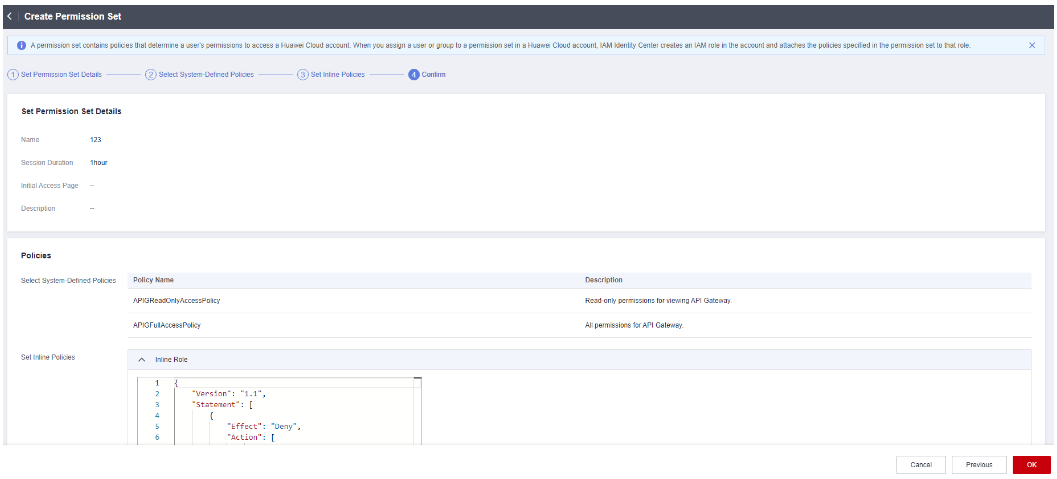
A permission set contains policies that determine a user's permissions to access a Huawei Cloud account. When you assign a user or group to a permission set in a Huawei Cloud account, IAM Identity Center creates an IAM role in the account and attaches the policies specified in the permission set to that role.

① Set Permission Set Details — ② Select System-Defined Policies — ③ Set Inline Policies — ④ Confirm

Type ○ Use inline policy
● Do not use

Step 8 In the **Confirm** step, confirm the configuration and click **OK** in the lower right corner.

Figure 3-9 Confirming the configuration



A permission set contains policies that determine a user's permissions to access a Huawei Cloud account. When you assign a user or group to a permission set in a Huawei Cloud account, IAM Identity Center creates an IAM role in the account and attaches the policies specified in the permission set to that role.

1 Set Permission Set Details
2 Select System-Defined Policies
3 Set Inline Policies
4 Confirm

Set Permission Set Details

Name	123
Session Duration	1hour
Initial Access Page	--
Description	--

Policies

Select System-Defined Policies

Policy Name	Description
APIGReadOnlyAccessPolicy	Read-only permissions for viewing API Gateway.
APIGFullAccessPolicy	All permissions for API Gateway.

Set Inline Policies

Inline Role

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
```

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

4 Associating Accounts with Users 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.

Procedure

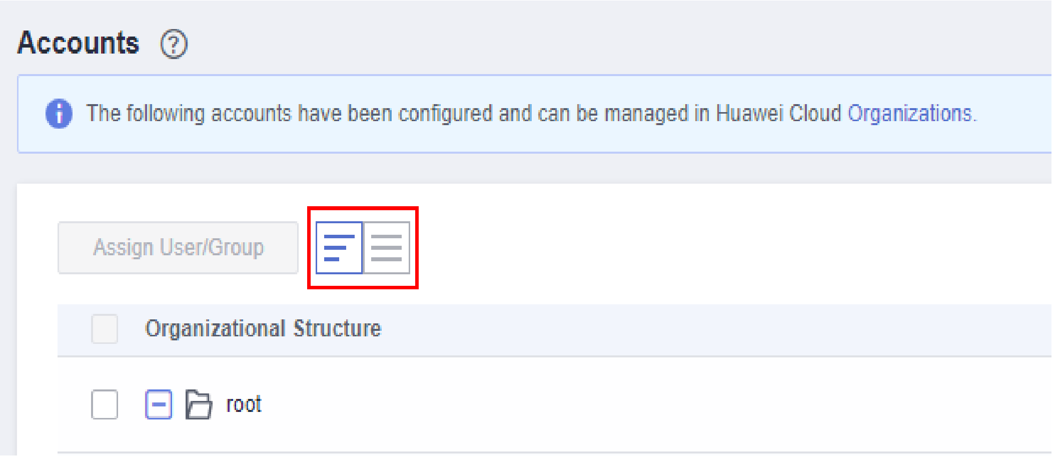
Step 1 Log in to the **Huawei Cloud console**.

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

Step 3 In the navigation pane on the left, 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 4-1 Account view



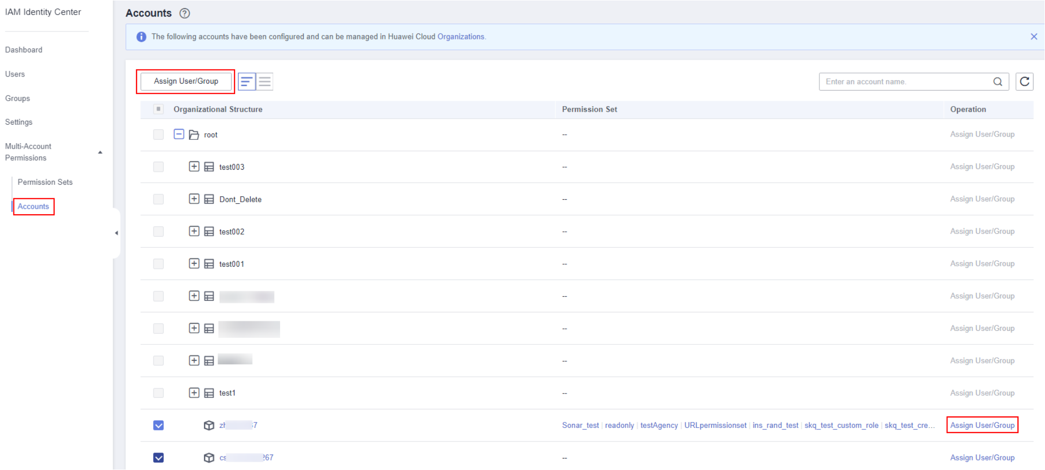
Accounts ⓘ

The following accounts have been configured and can be managed in Huawei Cloud Organizations.

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 4-2 Selecting accounts

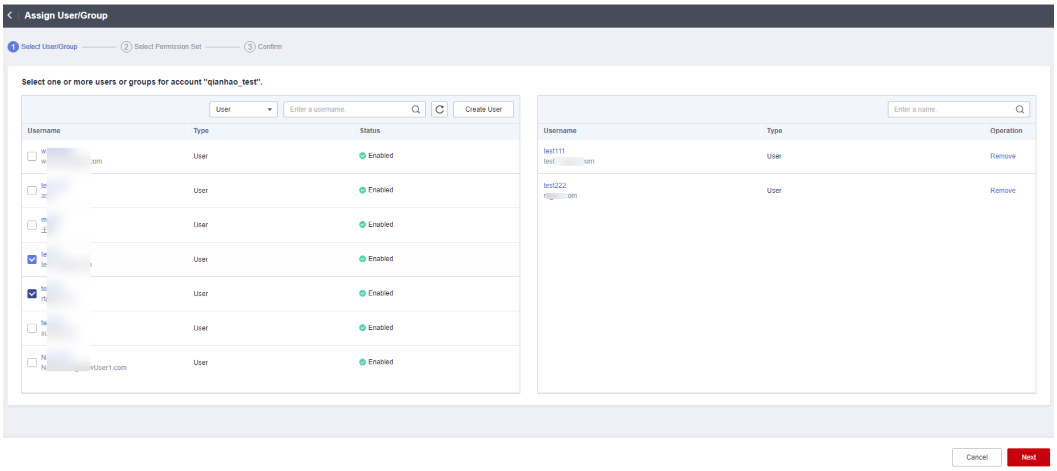


The following accounts have been configured and can be managed in Huawei Cloud Organizations.

	Organizational Structure	Permission Set	Operation
□	root	--	Assign User/Group
□	test003	--	Assign User/Group
□	Dont_Delete	--	Assign User/Group
□	test002	--	Assign User/Group
□	test001	--	Assign User/Group
□	[redacted]	--	Assign User/Group
□	[redacted]	--	Assign User/Group
□	[redacted]	--	Assign User/Group
□	test1	--	Assign User/Group
☑	[redacted]	Sonar_test | readonly | testAgency | URLpermissionset | ins_rand_test | skq_test_custom_role | skq_test_cre...	Assign User/Group
☑	[redacted]	--	Assign User/Group

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

Figure 4-3 Selecting one or more users/groups



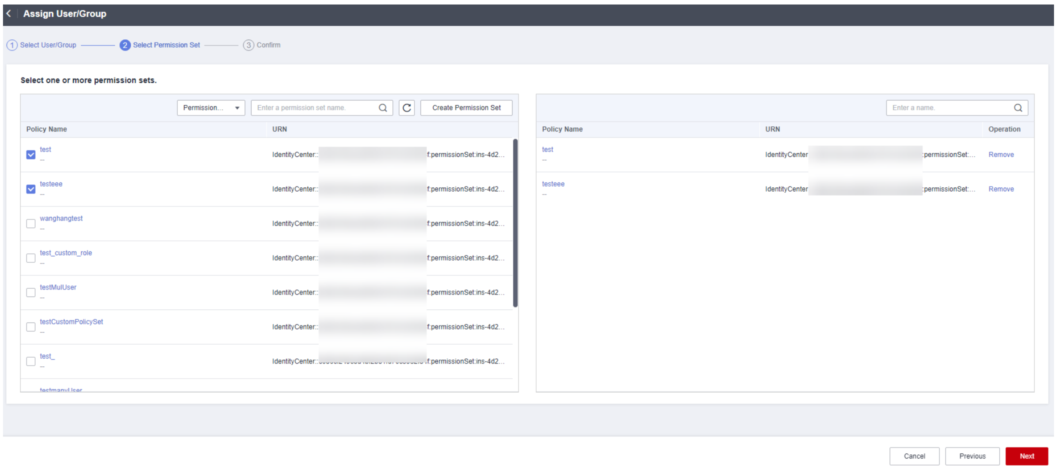
Select one or more users or groups for account "qianhao_test".

	Username	Type	Status
□	[redacted]	User	Enabled
□	[redacted]	User	Enabled
□	[redacted]	User	Enabled
☑	[redacted]	User	Enabled
☑	[redacted]	User	Enabled
□	[redacted]	User	Enabled
□	[redacted]	User	Enabled

Username	Type	Operation
test111 test[redacted]om	User	Remove
test222 [redacted]om	User	Remove

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

Figure 4-4 Selecting one or more permission sets



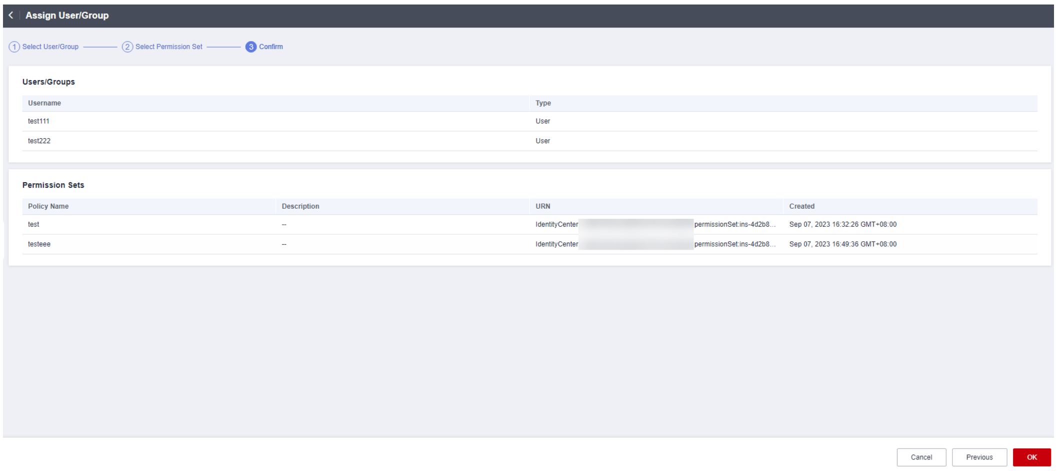
Select one or more permission sets.

	Policy Name	URN
☑	test --	IdentityCenter:[redacted]f:permissionSet:ins-4d2...
☑	testeee --	IdentityCenter:[redacted]f:permissionSet:ins-4d2...
□	wanghangtest --	IdentityCenter:[redacted]f:permissionSet:ins-4d2...
□	test_custom_role --	IdentityCenter:[redacted]f:permissionSet:ins-4d2...
□	testMulUser --	IdentityCenter:[redacted]f:permissionSet:ins-4d2...
□	testCustomPolicySet --	IdentityCenter:[redacted]f:permissionSet:ins-4d2...
□	test_ --	IdentityCenter:[redacted]f:permissionSet:ins-4d2...
	testmanyUser	

Policy Name	URN	Operation
test --	IdentityCenter[redacted]:permissionSet:...	Remove
testeee --	IdentityCenter[redacted]:permissionSet:...	Remove

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

Figure 4-5 Confirming configurations



Users/Groups

Username	Type
test111	User
test222	User

Permission Sets

Policy Name	Description	URN	Created
test	--	IdentityCenter[redacted]permissionSet:ins-4d2b8...	Sep 07, 2023 16:32:26 GMT+08:00
testeee	--	IdentityCenter[redacted]permissionSet:ins-4d2b8...	Sep 07, 2023 16:49:36 GMT+08:00

----End

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

After associating member accounts of an organization with an IAM Identity Center user and permission sets, you can use the IAM Identity Center username and password to log in to the console through the user portal URL and access resources according to the permissions included in the associated permission sets.

Procedure

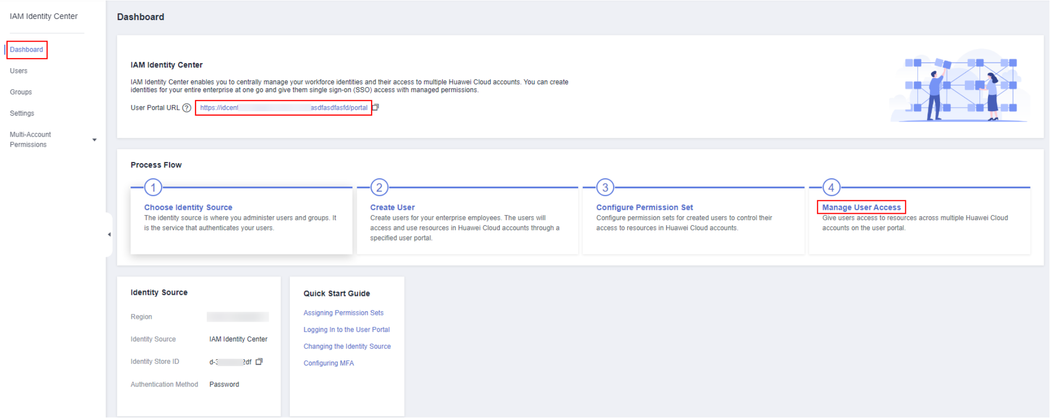
Step 1 Log in to the **Huawei Cloud console**.

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 5-1 User portal URL



IAM Identity Center

- Dashboard
- Users
- Groups
- Settings
- Multi-Account Permissions

Dashboard

IAM Identity Center

IAM Identity Center enables you to centrally manage your workforce identities and their access to multiple Huawei Cloud accounts. You can create identities for your entire enterprise at one go and give them single sign-on (SSO) access with managed permissions.

User Portal URL ⓘ https://idcent[redacted]asdfasdfasfd/portal

Process Flow

1. Choose Identity Source
   The identity source is where you administer users and groups. It is the service that authenticates your users.
2. Create User
   Create users for your enterprise employees. The users will access and use resources in Huawei Cloud accounts through a specified user portal.
3. Configure Permission Set
   Configure permission sets for created users to control their access to resources in Huawei Cloud accounts.
4. Manage User Access
   Give users access to resources across multiple Huawei Cloud accounts on the user portal.

Identity Source

Region	[redacted]
Identity Source	IAM Identity Center
Identity Store ID	d-3[redacted]2df
Authentication Method	Password

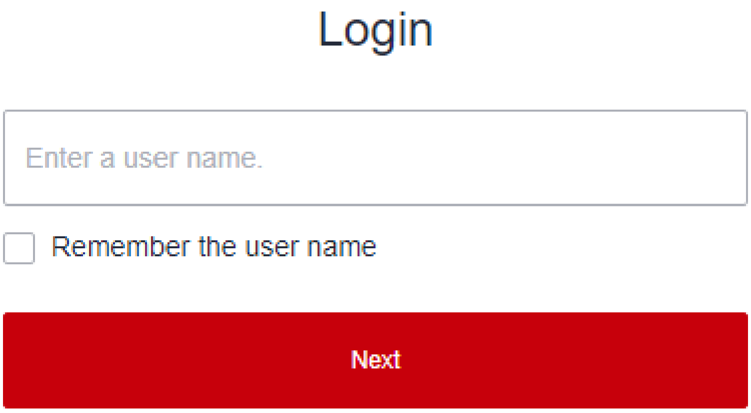
Quick Start Guide

- Assigning Permission Sets
- Logging In to the User Portal
- Changing the Identity Source
- Configuring MFA

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.

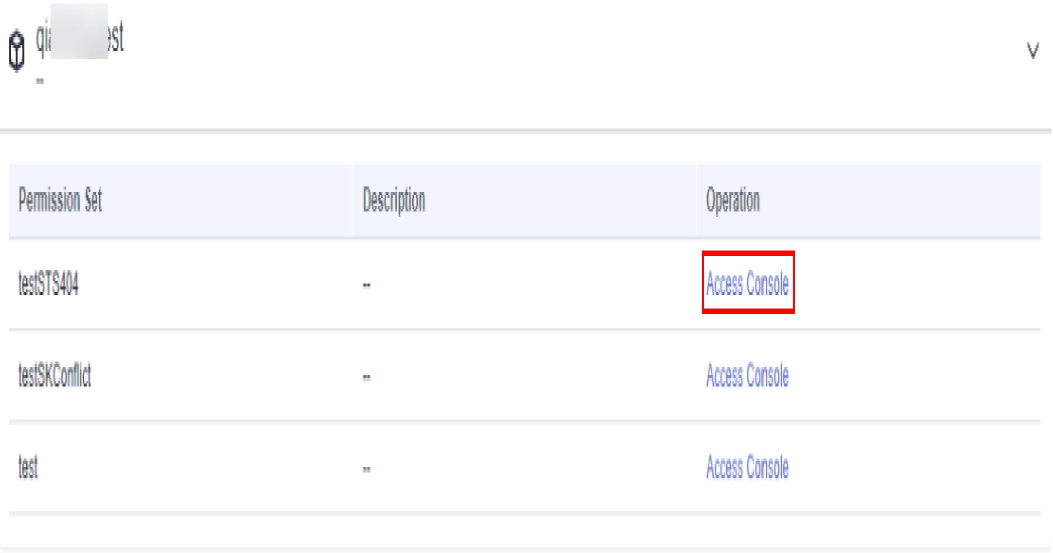
Figure 5-2 Login



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 5-3 Accessing resources



qi[redacted]st
--

Permission Set	Description	Operation
testSTS404	--	Access Console
testSKConflict	--	Access Console
test	--	Access Console

----End

6 Change History

Released On	Description
2023-08-30	This issue is the first official release.