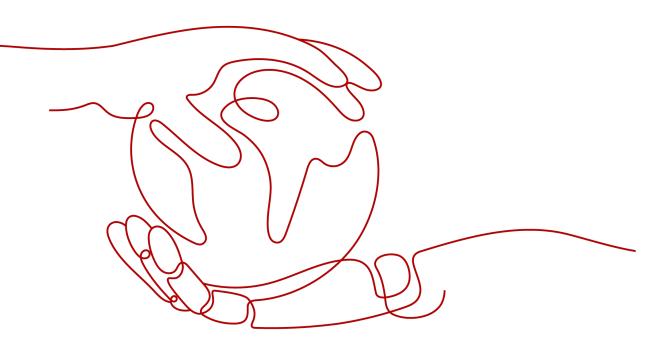
IAM Identity Center

User Guide

 Issue
 01

 Date
 2024-02-20





HUAWEI TECHNOLOGIES CO., LTD.

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

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

Trademarks and Permissions

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

Notice

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

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

Security Declaration

Vulnerability

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

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

For vulnerability information, enterprise customers can visit the following web page: <u>https://securitybulletin.huawei.com/enterprise/en/security-advisory</u>

Contents

1 User Management	1
1.1 Creating Users	1
1.2 Logging In as an IAM Identity Center User and Accessing Resources	4
1.3 Managing Users	6
1.4 Deleting Users	11
1.5 Configuring the Duration of the User Portal Session	12
2 Group Management	14
2.1 Creating a Group	14
2.2 Adding Users to or Removing Users from a Group	
2.3 Deleting a Group	17
3 Multi-Account Permissions Management	19
3.1 Registering a Delegated Administrator	19
3.2 Permission Sets	
3.2.1 Creating a Permission Set	20
3.2.2 Viewing or Modifying a Permission Set	23
3.2.3 Deleting a Permission Set	25
3.2.4 Managing Permission Set Tags	26
3.3 Accounts	
3.3.1 Associating Accounts with Users/Groups and Permission Sets	
3.3.2 Modifying Association with with Users/Groups and Permission Sets	
3.3.3 Removing Access Permissions and Permission Sets	
3.4 Attribute-based Access Control (ABAC)	
3.4.1 ABAC Overview and Configuration Process	
3.4.2 Enabling and Configuring Access Control Attributes	
3.4.3 Creating Permissions Policies for ABAC	
3.4.4 Supported User Attributes	43
4 Identity Source Management	45
4.1 Changing the Identity Source	
4.2 Customizing User Portal URL	
4.3 Configuring an External Identity Provider	
4.3.1 Overview	
4.3.2 Editing SAML 2.0 Configuration	

4.3.3 Enabling or Disabling SCIM Automatic Provisioning	51
4.3.4 Enabling Manual Provisioning	56
4.3.5 Managing Certificates	56
4.4 Supported Identity Providers	58
4.4.1 Microsoft Azure AD	58
4.4.2 Okta	59
5 IAM Identity Center Resetting	60
6 MFA Management	62
6.1 MFA Overview	62
6.2 MFA Authentication	62
6.2.1 Enabling MFA	63
6.2.2 Choosing an MFA Device Type	64
6.2.3 Configuring MFA Device Enforcement	64
6.2.4 Allows Users to Binding Their Own MFA Devices	65
6.3 MFA Configuration	65
6.3.1 Binding an MFA Device	65
6.3.2 Managing a User's MFA Device	67
7 Permissions Management	69
7.1 Creating an IAM User and Granting Permission to Use IAM Identity Center	69
7.2 Creating IAM Custom Policies for IAM Identity Center	70
8 Auditing	73
8.1 Key Operations Supported by CTS	73
8.2 Querying Real-Time Traces	77
9 Quotas	80
10 Change History	81

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 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

IAM Identity Center	Users ⑦							Create Us
Dashboard Users	Delete					Q Enter a username.		C
Groups	Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
Settings	chen	Enabled	chen	May 12, 2023 09:56:56 GMT+08:00	May 12, 2023 09:56:56 GMT+08:00	Manual	Manual	Delete
Multi-Account Permissions 🔻	33@3.com	S Enabled	33@3.com	Oct 26, 2023 11:16:23 GMT+08:00	Oct 26, 2023 17:02:05 GMT+08:00	Manual	Manual	Delete
	. 111	S Enabled	111	Dec 08, 2023 09:33:02 GMT+08:00	Dec 08, 2023 09:33:02 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.

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

Figure 1-2 Configuring basic information

< Create User			
1 Set User Details	(Optional) Add User to Groups (3) Confirm		
User Details			
* Username	Enter a username.	* Family Name	Enter a family name.
* Given Name	Enter a given name.	* Display Name	This is hysically the half name of the workforce user. Enter a dropkay name.
* Email Address	This email address will be used to receive password setup or reset instructions. email@example.com	Confirm Email * Address	unul@exunpix.com
* Password	Send an email to this user with password setup instructions. Orenerate a one-time password that you can share with this user.		
✓ Contact Method	is - Optional		
✓ Job-related Info	rmation - Optional		
✓ Address - Optic	nai		
			Cancel Nout

 Table 1-1
 User details

Parame ter	Description
Userna me	IAM Identity Center username. The value is user-defined and must be unique.
Passwor d	 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.
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.
Given Name	Given name of the user.

Parame ter	Description
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

Contra group taxes. C Center Group Contra arrows. Contrad arrows.	user "1234" to groups.				
		Enter a group name.	Q C Create Group		Enter a name.
- 12) - Remove	oup Name	Description	Group Name	Description	Operation
	m	-	13	-	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 1-4 Confirming user creation

< Create User		
① Set User Details ② (Optional) Add User to Groups ③ Continu		
User Details		
Username 27	Family Name Z	
Given Name n	Display Name 12	
Email Address Com		
Contact Methods - Optional		
Job-related Information - Optional		
 Address - Optional 		
Groups		
Group Name	Description	
lestwhgropu	-	
		Cancel Previous OK

----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 Permission Sets** and **Associating Accounts with IAM Identity Center 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 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.

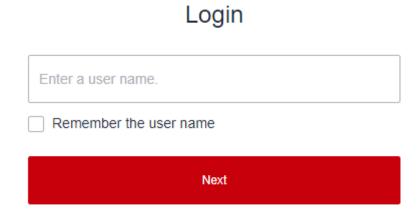
The user portal URL can also be obtained from the password setting instruction email sent to the user or from the one-time password page displayed when the user was created.

Figure 1	-5 User portal URL		
IAM Identity Center	Dashboard		
Users Groups Settings Multi-Account Permissions 🕶	LAM identity Center $\label{eq:constraint} Lambda (a) a constant manage your workforce identities and their isotenties to your workforce identities and their isotenties to your work workforce identities and a give a did give them image isgos of (SSO) accesses to your workforce identities to your workforce identities and the interval of the interva$	raccess to multiple Hugerel Cloud accounts. You can create or it in managed germacators.	
	The identity source is where you administer users and groups. It is Create the service that authenticates your users. and users.	3 3	
	Identity Source Quick Start Quide Repin Astgring Primision Site Astgring Primision Site Identity Tource UM Identity Center Cagging In the You Ford Identity Tource 0 4/2 Canage In the You Ford Authentication Mitting Personet Canage In the You Ford Canage In the You Ford	rial and a second s	

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 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.

gi ist	g	V
Permission Set	Description	Operation
testSTS404	-	Access Console
testSKConflict	-	Access Console
test		Access Console

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 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

Jsers ⑦							Create User
Delete					Q Enter a username.		C 😔
Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
chen	S Enabled	chen	May 12, 2023 09:56:56 GMT+08:00	May 12, 2023 09:56:56 GMT+08:00	Manual	Manual	Delete
33@3.com	S Enabled	33@3.com	Oct 26, 2023 11:16:23 GMT+08:00	Oct 26, 2023 17:02:05 GMT+08:00	Manual	Manual	Delete
. 111	📀 Enabled	111	Dec 08, 2023 09:33:02 GMT+08:00	Dec 08, 2023 09:33:02 GMT+08:00	Manual	Manual	Delete

- 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 other details about the user

User Details	dit							
Username	manual_user_test	User ID	e1482c64	15643a0ff1e8				
Family Name	testup	Given Name	manualup					
Display Name	manualtestup	Status	Enabled					
Email Address	m∈ .com ⊘Verified	Creation Mode	Manual					
Created	Jun 29, 2023 10:47:00 GMT+08:00	Updated	Aug 28, 2023 17:03:48 GN	/T+08:00				
✓ Contact Met	✓ Contact Methods - Optional Edit							
V Job-related Information - Optional Edit								
Address - C	V Address - Optional Edit							

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 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

sers ⑦							Create User
Delete					Q Enter a username.		C 🕲
Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
chen	Enabled	chen	May 12, 2023 09:56:56 GMT+08:00	May 12, 2023 09:56:56 GMT+08:00	Manual	Manual	Delete
33@3.com	Enabled	33@3.com	Oct 26, 2023 11:16:23 GMT+08:00	Oct 26, 2023 17:02:05 GMT+08:00	Manual	Manual	Delete
111	📀 Enabled	111	Dec 08, 2023 09:33:02 GMT+08:00	Dec 08, 2023 09:33:02 GMT+08:00	Manual	Manual	Delete

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

Figure 1-11 Disabling a user

< 33@3.com			Disable User Access Reset Password Delete User
User Details Ec	at		
Username	33@3.com	User ID	1d4c938 i1ac5f830c
Family Name	33@3.com	Given Name	33@3.com
Display Name	33@3.com	Status	© Enabled
Email Address	qir i.com OVerified	Creation Mode	Manual
Created	Oct 26, 2023 11:16:23 GMT+08:00	Updated	Oct 26, 2023 17:02:05 GMT+08:00

- **Step 6** In the dialog box that is displayed, 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.
- **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 1-12 Deleting a user

< 33@3.com			Disable User Access Reset Password Delete User
User Details	dt		
Username	33@3.com	User ID	164c938b- ac5f830c
Family Name	33@3.com	Given Name	33@3.com
Display Name	33@3.com	Status	C Enabled
Email Address	ginp .com Overified	Creation Mode	Manual
Created	Oct 26, 2023 11:16:23 GMT+08:00	Updated	Oct 26, 2023 17:02:05 GMT+08:00

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 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 1-13 Selecting a user

Jsers ⑦							Create User
Delete					Q Enter a username.		C 🕲
Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
Chen	Enabled	chen	May 12, 2023 09:56:56 GMT+08:00	May 12, 2023 09:56:56 GMT+08:00	Manual	Manual	Delete
33@3.com	Enabled	33@3.com	Oct 26, 2023 11:16:23 GMT+08:00	Oct 26, 2023 17:02:05 GMT+08:00	Manual	Manual	Delete
111	Enabled	111	Dec 08, 2023 09:33:02 GMT+08:00	Dec 08, 2023 09:33:02 GMT+08:00	Manual	Manual	Delete

Х

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

Figure 1-14 Resetting a password

< 33@3.com			Disable User Access Reset Password Detete User
User Details E	at		
Username	33@3.com	User ID	fd4c938b 1991ac5830c
Family Name	33@3.com	Given Name	33@3.com
Display Name	33@3.com	Status	📀 Enabled
Email Address	ginping9@h-partners.com OVerified	Creation Mode	Manual
Created	Oct 26, 2023 11:16:23 GMT+08:00	Updated	Oct 26, 2023 17:02:05 GMT+08:00

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

Figure 1-15 Selecting a password resetting method

Reset Password for User 33@3.com How do I reset this user's password? Send an email to the user with instructions for resetting the password Generate a one-time password and share the password with the user M Cancel

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 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 1-16 Selecting a user

sers ⑦							Create User
Delete					Q Enter a username.		C
Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
chen	Enabled	chen	May 12, 2023 09:56:56 GMT+08:00	May 12, 2023 09:56:56 GMT+08:00	Manual	Manual	Delete
33@3.com	Enabled	33@3.com	Oct 26, 2023 11:16:23 GMT+08:00	Oct 26, 2023 17:02:05 GMT+08:00	Manual	Manual	Delete
111	Enabled	111	Dec 08, 2023 09:33:02 GMT+08:00	Dec 08, 2023 09:33:02 GMT+08:00	Manual	Manual	Delete

- **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 1-17 Adding a user to groups

User Details	Edit					×
Username	33@3.com	Add User "33@3.c Select or create the groups to	om" to Groups which the user will be added. The user will int	nerit the permissions from the	e groups to access Huawei C	
Family Name	33@3.com					
Display Name	33@3.com	Q Ente	er a group name.		Q Enter a name.	
Email Address	qinping9@h-	Group Name	Description	Group Name	Description	Operation
Created	Oct 26, 2023	test	fsdfasd~! @#¥%&* ()	jijianggroup	-	Remove
		yijianggroup				
✓ Contact Me	ethods - Optic	123				
		25	-			
 ✓ Job-related 	d Information	□ _				
		gsdddfgsd				
✓ Address -	Optional Edit	GDFHGGF	-			
	_	GHHHHHGFFFFFFD				
Groups M	IFA Devices					
1 To assign	permissions to th		ОК	Cancel		
Add User to G		ove User from Groups				
Group 1	Name				Description	
fodfod						

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 1-18 Removing a user from groups

Groups MFA Devices Active Sessions		
To assign permissions to this user, add the user to a group that has permissions to access Huavei Cloud account	ts.	×
Add User to Groups Remove User from Groups		Q. Enter a group name.
Group Name	Description	Operation
Jjianggroup	-	Remove
V fedfed		Remove
Chen Chen	dtsad	Remove

----End

1.4 Deleting Users

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 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 1-19 Deleting a user

sers 💮							Create Use
Delete					Enter a username.		QC
Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
manual_user_test	Enabled	manualtestup	Jun 29, 2023 10:47:00 GMT+08:00	Aug 28, 2023 17:03:48 GMT+08:00	Manual	Manual	Delete
y ;o	Enabled	GD	Jun 29, 2023 11:07:36 GMT+08:00	Jun 29, 2023 11:07:36 GMT+08:00	Manual	Manual	Delete

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

----End

Batch Deleting 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 In the user list, select multiple users and click Delete above the list.

Figure 1-20 Batch deleting users

Isers ⑦							Create User
Delete					Enter a username.		Q C @
Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
manual_user_test	😋 Enabled	manualtestup	Jun 29, 2023 10:47:00 GMT+08:00	Aug 28, 2023 17:03:48 GMT+08:00	Manual	Manual	Delete
.550	C Enabled	GD	Jun 29, 2023 11:07:36 GMT+08:00	Jun 29, 2023 11:07:36 GMT+08:00	Manual	Manual	Delete
sonarTest	Enabled	sonarTest	Jun 29, 2023 14:36:58 GMT+08:00	Jun 29, 2023 14:36:58 GMT+08:00	Manual	Manual	Delete

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 reauthentication 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 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 left 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. You can also select **Custom duration** and enter a specific duration from 15 minutes to 129,600 minutes.

AM Identity Center	Settings ⑦
Dashboard Jsers	Details
Groups	URN dd4
Settings	Region
Multi-Account Permissions 🔻	
	Identity Source Management Authentication Session Settings Access Control Attributes
	Configure the maximum length of time that a user can be logged in before they must be re-authenticated.
	Maximum Session Duration Custom duration 30 min Maximum session duration: 90 days (129,600 min)
4	Save

Figure 1-21 Session settings

I

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 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

IAM Identity Center	Groups ⑦				Create Group
Dashboard Users	Delete			Q: Enter a group name.	C
Groups	Group Name	Description	Created By	Created	Operation
Settings	chen	dfsad	Manual	May 12, 2023 09:57:14 GMT+08:00	Delete
Multi-Account Permissions 🕶	test	fsdfasd-! @#¥%&* ()+))))))))(): " ?) () fssss	Manual	May 12, 2023 09:57:27 GMT+08:00	Delete

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 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

Groups ⑦				Create Group
Delete			Enter a group name.	QC
Group Name	Description	Created By	Created	Operation
test		Manual	Aug 23, 2023 10:57:37 GMT+08:00	Delete
test1	-	Manual	Aug 23, 2023 10:57:55 GMT+08:00	Delete

- 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

roup Name testGGG	Add Users to Select users to add to	Group "test this group.	GGG"					
ast Updated Sep 13, 2023 21:00:25 GMT+08:00		Enter a username.		QC		Enter a na	ame.	Q
	Username	Display Nam	е	Status	Username	Display Name	Status	Operation
Jsers in This Group	wanghang		:om	Enabled	test_mfa	asdf	Enabled	Remove
() Users in this group inherit access to any accounts that y	🖌 test_mfa			Enabled	test111	test1	Enabled	Remove
Add User to Group Remove User from Group	masen			Enabled				
Username	test111		1	Enabled				
	test222			Enabled				
	test209			Enabled				
	NewUser1		vU	Enabled				



Removing Users from a Group

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 **Groups**.
- **Step 4** In the group list, click a group name.

Figure 2-4 Selecting a group

Groups 💿				Create Group
Delete			Enter a group name.	QC
Group Name	Description	Created By	Created	Operation
test	-	Manual	Aug 23, 2023 10:57:37 GMT+08:00	Delete
test1	-	Manual	Aug 23, 2023 10:57:55 GMT+08:00	Delete

- **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

Group Details				
Group Name		Created Set	26, 2023 14:29:15 GMT+08:00	
Last Updated Sep 26, 2023 14:29:15 GMT+08:00		Description -	<u>e</u>	
Users in This Group				
Users in this group inherit access to any accounts to	hat you have assigned to this group.			×
Add Users to Group Remove Users from Grou	q		Enter	a username or display name. Q
Username	Display Name	Status	Email Address	Operation
33@3.com	33@3.com	Enabled	qinping9@h-partners.com	Remove
111	111	Enabled	1@1.com	Remove

- **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

Group Details						
Group Name		Created	Sep 26, 2023 14:29:15 GMT+08:0	10		
Last Updated Sep 26, 2023 14:29:15 GMT+08:00		Description	- 🖉			
Users in This Group						
Users in this group inherit access to any accounts that you have ass	igned to this group.					×
Add Users to Group Remove Users from Group					Enter a username or display name.	QC
Username	Display Name	Status		Email Address		Operation
✓ 33@3.com	33@3.com	Enabled		qinping9@h-partners.c	om	Remove
☑ 111	111	Enabled		1@1.com		Remove

----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 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

iroups ⑦				Create Group
Delete			Enter a group name.	QC
Group Name	Description	Created By	Created	Operation
test		Manual	Aug 23, 2023 10:57:37 GMT+08:00	Delete
test1	-	Manual	Aug 23, 2023 10:57:55 GMT+08:00	Delete
qwerqwer	-	Manual	Aug 23, 2023 16:20:06 GMT+08:00	Delete
dmedmememe	-	Manual	Aug 23, 2023 16:20:12 GMT+08:00	Delete

----End

Batch Deleting Groups

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

Figure 2-8 Batch deleting groups

Groups ⑦				Create Group
Delete			Enter a group name.	QC
Group Name	Description	Created By	Created	Operation
🗹 test	-	Manual	Aug 23, 2023 10:57:37 GMT+08:00	Delete
✓ test1	-	Manual	Aug 23, 2023 10:57:55 GMT+06:00	Delete
qwerqwer		Manual	Aug 23, 2023 16:20:06 GMT+08:00	Delete
dwedwewewe		Manual	Aug 23, 2023 16:20:12 GMT+08:00	Delete

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

----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 member accounts in your organization to extend the ability to manage IAM Identity Center.

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** Choose **Settings** in the left navigation pane.
- **Step 4** On the **Management** tab, click **Register**.
- **Step 5** In the displayed dialog box, select a member account and click **OK**.

Settings 🕜					
Details	Register Delegated Ac	iministrator		x	
URN d- cd4 Region	This operation will delegate permissions to users in this permissions for the delegat Identity Center administrativ Identity Center, registering administrators, managing a managing permission sets in	member account. All user ed administrator account o ve tasks from the account, other member accounts as ssignments to the manage	s who have sufficient an perform all IAM except for: deleting IAM delegated ment account, and		
Identity Source Management Authentication Session S			n account name. Q		
Delegated Administrator ⑦	Account Name	ID 0013344c7	155bf9b255f		Enter an account name. Q
Account Name	• test06	08830e5f6a	2e7ead5423	Time	Operation
test10	O test08	119b94feda	209a32aec6	4 16:42:17 GMT+08:00	Deregister
) test11	11a2cef9f3i	dc834c63e		
Delete IAM Identity Center Configuration	onew-org_account	13/6209300	3b984c257b		
This operation will delete all data in the IAM Identity Center configuration, include	test09	2908e770e	047573359	M Identity Center as your identity sou	rce, this operation will also delete all users and groups from IAM Identity
Center You can delete this configuration if you need to create a new configuratio		OK Cancel			

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

RN d-9fbb718cd4	×		
igion	Administrator?		
entity Source Management Authentication Session Settings	If you deregister this account as a delegated administrator, all users in this account will lose administrative access to IAM Identity Center from this account. Deregister the delegated administrator?		
Delegated Administrator ⑦ Register	OK Cancel		Enter an account name. Q
Account Name	Account ID	Delegation Time	Operation
test10	0013344(5bf9b255f	Jan 17, 2024 16:42:17 GMT+08:00	Deregister
Delete IAM Identity Center Configuration This spectra delete all data in the IAM Identity Center configuration, including use Center You can delete bits configuration if you need to create a new configuration from Deater		lf you are using IAM Identity Center as your Identity sou	rce, this operation will also delete all users and groups from IAM Identity

----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 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
-----------------------	----------------

IAM Identity Center	Permi	ssion Sets ⑦						Create Permis	ision Set
Dashboard						Permission	Enter a permission set name.	Q	С
Users	Pe	ermission Set Name	Description	URN	Attachment Status		Created	Operation	
Groups	te	stSTS404	-	IdentityCenter:::c086ct249ced4bt2b811d70c3932t84f.permissionSet1	Attached		Jul 27, 2023 20:44:52 GMT+08:00	Delete	
Settings Multi-Account	ter	stSKConflict	-	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84f.permissionSet1	Attached		Jul 27, 2023 20:51:58 GMT+08:00	Delete	
Permissions	ber	st	-	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84f.permissionSet1	Attached		Jul 31, 2023 11:50:07 GMT+08:00	Delete	
Permission Sets	fat	faagfargarg	-	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84f.permissionSet1	Not attached		Jul 31, 2023 17:19:28 GMT+08:00	Delete	
Accounts	ber	st1	-	IdentityCenter::c088cf249ced4bf2b81fd70c3932f84f.permissionSet1	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 3-4 Setting permission set details

Create Permissi	on Set					
A permission set con	tains policies that determin	e a user's permiss	ions to access	a Huawei Cloud ao	count. When you assign a user or group to a permission set in a Huawei Cloud account, UAM identity Center creates an UAM role in the account and attaches the policies specified in the permission set to that role.	×
Specify Details	2) Set Policy	(3) Confir	m			
* Name	123					
* Session Duration	th 4h	8h	12h	Custom		
	Custom duration		8			
Initial Access Page	Enter the initial access	page URL.				
Description	Enter a description.					
		0/1,024				
					Ca	Incel Next

Table 3-1 Permission set of	details
-----------------------------	---------

Parame ter	Description
Name	Name of a permission set. The value is user-defined and must be unique.
Session Duratio n	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.
Descript ion	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

< Create Permis	ssion Set						
A permission set	contains policies that determine a user's permissions to	access a Huawei Cloud account. When you assign a us	er or group to a permission set in a Huawei Cloud account,	AM Identity Center creates an IAM role in the account and attache	s the policies specified in the permission set to that role.		×
Specify Details —	(3) Confirm						
Identity Policy	Identity policies can be customized and give you more	e granular, more flexible control of your resources.					
V System-defined IAM provides sy		If cloud services. You can directly choose from these IAM	system-defined policies, but cannot modify them.				
Custom identity Custom identity Policy View	policies Not set policies can be created to supplement system-defined Visual estor JSON	identity policies for fine-grained permissions control.					
Policy Content	Allow Allow Deny	C Select service	C Select action	Cptional) Select resource	(Optional) Add request condition	0 0	
	Add Permissions						
 Custom policies Custom policies 	Not set	for fine-grained permissions control.					
							_

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

Figure 3-6 Confirming configurations

Create Permission Set			
A permission set contains policies that determine a user's permissions to access a Huawe	ei 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.	×
Specify Details Set Policy Set Policy			
Specify Details			
Name 123			
Session Duration 1h			
Initial Access Page			
Description			
System-defined policies			
Policy Name	Туре	Description	
 Organizations ReadOnlyAccess 	Policy	Read-only permissions for Organizations Manager	
 OrganizationsReadOnlyAccessPolicy 	Identity policy	Read-only permissions for Organizations Manager.	
Custom identity policies			
1 { 2 "Version": "5.0",			
3 "Statement": [4 {			
5 "Effect": "Allow",			

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 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

< 123						Edit Permission Set	Delete Permission Set
Permission Set De	atails						
Name	123			Session Duration	1h		
Initial Access Page	-			Created	Jan 16, 2024 16:24:51 GMT+08:00		
URN	IdentityCenter::e74e043fab78	275/ps-435e429	91840a97c5	Attachment Status	Attached		
Description	-						
IAM system-de IAM system-de	fined policies are standaione policies that are created and managed by IAM defined policies (2)	. Different types of IAM system	m-defined policies enab	ie you to grant predefined	permissions for many common use cases.		×
							С
Policy N	ame	Policy Type	Description				
✓ Organiza	tionsReadOnlyAccessPolicy	Identity policy	Read-only permission	ons for Organizations Man	ager.		
✓ Organiza	tions ReadOnlyAccess	Policy	Read-only permissio	ons for Organizations Man	ager		
✓ Custom ident	ity policy (set)						
 Custom polic 	y (set)						

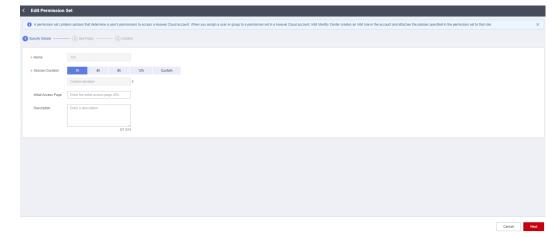
----End

Editing a Permission Set

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** 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

< Edit Permission Set	
A permission set contains policies that determine a scen's permissions to access a Haused Elocal account. When you assign a scen's pranticion set in a Haused Elocal account, MM identity Center creates as MM role in the account and attaches the policies specified in the permission rel to that non-	×
Speed Details	
ldenthy Präcy 💿 Identhy policies can be customesel and give you more granular, more Seruble control of your resources.	
V bythem-defined paticies Bet UM provide system-defined paticies that define the common actions of cloud services. You can directly choose from these IAM system-defined patices, but cannot modify them.	
Cuttom identity policies are be created to supplement system-defined identity policies for time-gramed permissions control	
Cuttom policies Set	
Canol Previou	Next

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

----End

Updating Permission Sets

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 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

Permissions Accounts Tags			
The following Huawei Cloud accounts use this permission set. To update this permission set in one or more Huawei Cloud account	nts, select the accounts and click Update.		×
Update		Q Enter a keyword.	C
Account Name	Permission Set Status		Operation
	Up to date		Update

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 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

IAM Identity Center	Permission Sets ②					Create Permission Set
Dashboard Users					Permission • Q 123	×C
Groups	Permission Set Name	Description	URN	Attachment Status	Created	Operation
Settings	123	-	IdentityCenter::e7	Ibcffc:permissionSet.ins 9 Not attached	Jan 16, 2024 16:24:51 GMT+08:00	Edit Delete
Multi-Account Permissions A						
Permission Sets						
Accounts						

----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

• The following basic naming and usage requirements apply to the key and value of a tag:

Tag key:

- Cannot be left blank.
- Contains 1 to 128 characters.
- Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF).

Tag value:

- Can be left blank.
- Contains 1 to 225 characters.
- Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF).
- 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 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 **Predefined Tags**.

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

Permissions Accounts Tags Add Tags you can still create for this permission set: 3	Edit Tag X If is nonmended that you use TMS's predefined top function to add the same tag to different colour resources. Wee predefined tags C	C
Køy S	allieren uoda resources. Vere produined lags (Key s	Operation Edit Dulete
sd	Value s	Edit Delete
sdada	OK Cancel	Edit Delete
dfssssssssffsa		Edit Delete

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

Permissions Accounts Tags Add Tags you can still create for this permission set: 3	A Delete Tag			C
Key	Delete the following tag? Deleted tags cannot be recovered.		- 1	Operation
5	Кеу	Value	1	Edit Delete
sd	\$	\$		Edit Delete
sdada	ок	Cancel		Edit Delete
dfssssssssffsa				Edit Delete

----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. You can manage them on the **Organizations console**.

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 3-15 Account view

Accounts ⑦
The following accounts have been configured and can be managed in Huawei Cloud Organizations.
Assign User/Group
Organizational Structure
- 🔁 root
+ = OU2

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

counts ⑦		
The following accounts have been configured and can be managed in Huawei Cloud Organizations.		
Assign User/Group		Q Enter an account name.
Organizational Structure	Permission Set	Operation
📄 🖻 root	-	Assign User/Group
1 目 002		Assign User/Group
1	-	Assign User/Group
★ E OU4-test	-	Assign User/Group
* E OU3	-	Assign User/Group
+ E testig	-	Assign User/Group
		Assign User/Group
€	-	Assign User/Group
+ = *****	-	Assign User/Group
	-	Assign User/Group
+ E AA test001		Assign User/Group
✓ ⑦ test06	-	Assign User/Group
✓ Ŷ test08	11111 HWServiceCatalogEndUserAccess	Assign User/Group

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

< Assign User/Group Select one or more users or a unt "test06" User v Q. Enter a C Create User Status Type chen chen chen chen 😌 Enabled User User 33@3.com 33@3.com 33@3.com User 😋 Enabled Use 111 111 Use 😋 Enable Cancel

Figure 3-17 Selecting one or more users/groups

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

lect one or more permission	n sets.				
	Permission Enter a permission set name. Q	C Create Permission Set			Enter a name.
olicy Name	URN		Policy Name	URN	Oper
test	IdentityCenter::	t permissionSet ins-4d2	test 	Identity Center	permissionSet Remo
testeee	IdentityCenter:	t permissionSet ins-4d2	testeee	IdentityCenter	permissionSet Remo
wanghanglest	IdentityCenter:	tpermissionSet ins-4d2			
test_custom_role	IdentityCenter:	t permissionSet ins-4d2			
testMulUser	IdentityCenter:	tpermissionSet ins-4d2			
testCustomPolicySet	IdentityCenter:	t permissionSet ins-4d2			
test_	IdentityCenter:	tpermissionSet ins-4d2			
factmanyl loar					

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

Figure 3-19 Confirming configurations

Visity Name Description URN Created etd - Identify-Center geentsconfect tro-44288. Sep 07, 2033 19.32.24 GMT 19.05						
set11 User ss222 User						
ber Center rmsson 545 Poly Center Poly Center Center rdig Amage Decorption URA Center Center rdig Amage						
Immission Sets URN Created Values Description URN Created etd - MarthyCenter permissionSet in 44288. 69 97, 2032 19.322 40.47749.09						
Visity Name Description URM Created ed - Identify-Center permissionSet III = 442386 69 (P) 303 19.322 60 MIT-10.00	est222		User			
Visity Name Description URM Created ed - Identify-Center permissionSet III = 442386 69 (P) 303 19.322 60 MIT-10.00						
eti - IdentityCenter permissonSet.ins-402bil	ermission Sets					
	Policy Name	Description	URN		Created	
- IdentityCenter permission/Set/Ins-4028 Sep 07, 2023 16 48 36 OWT-405 00	est	-	Identity Center	permissionSet:ins-4d2b8	Sep 07, 2023 16:32:26 GMT+08:00	
	esteee	88	Identity Center	permissionSet:ins-4d2b8	Sep 07, 2023 16:49:36 GMT+08:00	

----End

3.3.2 Modifying Association with 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 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 3-20 Account view

Accounts ⑦
The following accounts have been configured and can be managed in Huawei Cloud Organizations.
Assign User/Group
Organizational Structure
🗖 🔁 root
+ = OU2

- **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

< test06		
Account Details		
Name test06		
ID 08830e	ead5423	
Users/Groups Permission	Sets	
() The following users and grou	ps in IAM Identity Center can access this Huawei Cloud	account from the user portal.
Assign User/Group Cha	Inge Permission Set Remove Access Permission	ons
Name		Permission Set

- 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
J							

Account Details			
Name gia st			
ID c088cf24f :3932f84f			
Users/Groups Permission Sets			
The following users and groups in IAM Identity Center can access this Huar	vel Cloud account from the user portal.		×
Assign User/Group Change Permission Set Remove Access			Enter a username or group name. Q
Vame	Permission Set	Туре	Operation
V w/ ng	TestORG	User	Change Permission Set Remove Access Permissions
💙 to en	testSTS404 test testSKConflict	User	Change Permission Set Remove Access Permissions

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

< test06		
Account Details		
Name test06		
ID 08830e5 37ead5423		
Users/Groups Permission Sets Permission sets define the level of access permissions assigned to users and groups in IAM Identity Center for this Huavei Cloud acceut. Huavei Cloud acceut to reapply or reet your permissions in IAM.	Permission sets are stored in IAM Identity Center and displayed in the account as IAM agencies.	You can update any permission sets associated with this $ \times$
Remove		Enter a permission set name. Q
Permission Set Name	Description	Operation
☑ 123	-	Remove Update
✓ fas	afs	Remove Update

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 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 3-24 Account view
Accounts ⑦
The following accounts have been configured and can be managed in Huawei Cloud Organizations.
Assign User/Group
Organizational Structure
📄 🖻 root

- **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

< test06			
Account Details			
Name test06			
ID 08830e51 'ead5423			
Users/Groups Permission Sets The following users and groups in IAM Identity Center can a	ccess this Huawei Cloud account from the user portal.		×
Assign User/Group Change Permission Set	Remove Access Permissions		Enter a username or group name. Q
Name Name	Permission Set	Туре	Operation
✓ chen	123	User	Change Permission Set Remove Access Permissions
✓ 33@3.com	123	User	Change Permission Set Remove 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.

test06		
count Details		
me test06		
08830e5%a334a3895dcb22e7ead5423		
ers/Groups Permission Sets		
	ps in IAM Identity Center for this Huavei Cloud account. Permission sets are stored in IAM Identity Center and displayed in the account as IAM agencies. You can update	any permission sets associated with this
Permission sets define the level of access permissions assigned to users and group		any permission sets associated with this nicsion set name. $\ensuremath{\mathbb{Q}}$
Permission sets define the level of access permissions assigned to users and group Huawei Cloud account to reapply or reset your permissions in IAM.		
Permission sets define the level of access permissions assigned to users and prove Huaveie Cloud acceure to reapply or reset your permissions in IAM. Remove Update	Enter a peri	nission set name. Q

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.

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

 Table 3-2 ABAC configuration process

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 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 left navigation pane.
- Step 4 Click Enable on the Access Control Attributes tab.

i igure 5			
IAM Identity Center	Settings ⊘		
Dashboard Users	Details		
Groups	URN d- 32		
Settings	Region		
Multi-Account Permissions 🔻			
	Identity Source Management Au	herification Session Settings Access Control Attributes	
	Assign access permissions to users based	n the attribute key-value pairs.	
	Enable		Enter an attribute key or value. Q
	Attribute Key	Attribute Value	Operation
		(1) To grant access based on user attributes, enable this feature.	

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 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 left 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

etails		
RN d- 32		
egion		
tentity Source Management Authentication Session Settings Access Control Al	Add Access Control Attributes	
entity Source Management Authentication Session Settings Access Control Al Assign access permissions to users based on the attribute key-value pars.		
	Add Access Control Attributes	ther an altitude key or value. Q

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 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 left 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

ettings ⑦				
Details				
URN d- 332				
Region				
Identity Source Management Authentication Session Settings	Access Control Attributes			
Assign access permissions to users based on the attribute key-value pairs.			×	
	Edit Access Control Attr	butes	^	
Add Delete Disable Attributes you can still add: 19	Attribute Key	Attribute Value		Enter an attribute key or value. Q
Add Delete Disable Attributes you can still add: 19 Attributes Key	Attribute Key test1		×	Enter an attribute key or value. Q Operation
	test1	Attribute Value S(user.name)	×	
Attribute Key		Attribute Value S(user.name)	×	Operation

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

ings 🕜				
etails				
RN d-2 32				
egion				
Mentity Source Management Authentication Session Settings	Access Control Attributes			
entity Source Management Authentication Session Settings Assign access permissions to users based on the attribute key-value pairs.			×	
	Access Control Attributes	ntrol Attributes	×	Enter an attribute key or value.
Assign access permissions to users based on the attribute key-value pars. Add Deline Disable Attributes you can still add. 18			×	
Assign access permissions to users based on the abbude key-value pairs. Add Osake Disable Abbudes you can still add: 18 Abbudes Key	A Delete Access Co		×	Operation
Asign access permissions to users based on the attribute key-value pars. Add Delete Delable Attributes you can still add. 18	Delete Access Con	ibute?	*	

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

Settings ⑦			
Details			
URN d-2 32			
Region			
Identity Source Management Authentication Session Settings Access Control Attributes • Asign access permissions to users based on the attribute key-value pairs.	Delete Access Control J Delete the following attributes		
Add Delete Disable Attributes you can still add: 18	Attribute Key	Attribute Value	Enter an attribute key or value. Q C
Attribute Key	test1	\${user:name}	Operation
V Autobale Key	test2	\$(user.email)	Edit Delete
-	ок	Cancel	
V test2			Edit Delete

----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 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 left 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**.

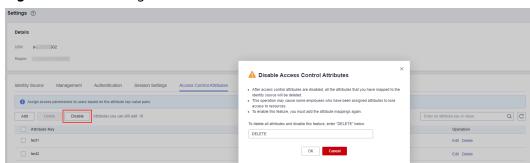


Figure 3-32 Disabling access control attributes



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/*tagkey*} 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	\${path:userName}
provider	\${path:name.familyName}
	\${path:name.givenName}
	\${path:displayName}
	\${path:nickName}
	<pre>\${path:emails[primary eq true].value}</pre>
	<pre>\${path:addresses[type eq "work"].streetAddress}</pre>
	<pre>\${path:addresses[type eq "work"].locality}</pre>
	<pre>\${path:addresses[type eq "work"].region}</pre>
	<pre>\${path:addresses[type eq "work"].postalCode}</pre>
	<pre>\${path:addresses[type eq "work"].country}</pre>
	<pre>\${path:addresses[type eq "work"].formatted}</pre>
	<pre>\${path:phoneNumbers[type eq "work"].value}</pre>
	\${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). You can use IAM identity providers (IdPs) to manage user identities outside of Huawei Cloud. 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. The IAM Identity Center administrator does not need to re-assign passwords.

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

Details		
URN d- d4	14	
Region		
rtogion		
Identity Source	Management Authentication Session Settings Access Control Attributes	
Identity Source	IAM Identity Center Change to external identity provider ⑦ You will manage all users and groups in IAM Identity Center. Users log in through the IAM Identity Cent	er user po
Authentication Method	Password	
Provisioning Method	Direct	
Identity Store ID	d- ::d4	
User Portal URL	Default URL: https://idcenter. 718cd4/portal	
	Custom URL	
	-	

Figure 4-1 Changing to an 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.

- 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.

Cancel Next

Figure 4-2 Configuring an identity provider

< Change Identity Source	
Configure Identity Provider (2) Confirm	
Target identity Source	External identity provider
Service Provider Details ⑦	<u>≜Download Meladula Fie</u>
IAM Identity Center User Portal URL	https://dce portal 0
IAM Identity Center Assertion Consumer Service (ACS) URL	https:// 3x24426 0
IAM Identity Center Issuer URL	https:// ecd86 0
Identity Provider Details ③	
IdP SAML Metadata Select File	
Choose an XML file. Maximum	n file store: 50 KB
🖹 beta1idp.xml	
or	
Identity Provider Login URL Enter a URL.	
Identity Provider Issuer URL Enter a URL.	
Identity Provider Certificate Select File	

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

< Change Identity So	urce
(1) Configure Identity Provider	O contra
Identity Source Details	
Target identity Source	Edemai letetiy provider
Service Provider Metadata	167 9340 (Mediada) Balantilo an La fuenza (2010)
Review and Confirm	
You are changing yo IAM Identity Center IAM Identity Center IAM Identity Center IAM Identity Center You must manage yi You must add (provi modify them in your ide	sequences of the processing learning le
	Cencel Previous OK

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 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 left 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
Settings
©

Details	
URN d- :c	м
Region	
Identity Source	Management Session Settings Access Control Attributes
Identity Source	External identity provider Change to IAM Identity Center 🕥 You will manage all users and groups in an external identity provider. Users log in on your identity provider page and are redirected to the IAM Identity Center user portal. After users log in to the Huawel Cloud access portal, they can access the Huawel Cloud accounts assigned to them.
Authentication Method	SAML 2.0 Modify SAML 2.0 Configuration
Provisioning Method	SCIM automatic provisioning Manual provisioning
Identity Store ID	64
User Portal URL	Default URL: https://dcer d-98bb/718cd4/portal
	Custom URL
	https://docenterwnv Enter a subdomain. doutal
Save	

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

<	< Change Identity Source		
	Identity Source Details		
	Target Hently Source VMI Kently Center		
	Preview and Continue Over the Machine Structure drive and Read Structure draws: Over the Machine Structure drive and Machine Structure draws: Over the Machine Structure drive and the Machine Structure draws: Over the Machine Structure draws and an approximation of the Machine Structure draws: Over the Machine Structure draws and approximation of the Machine Structure draws: Over the Machine Structure draws and approximation of the Machine Structure draws: Over the Machine Structure draws and approximation of the Machine Structure draws: Over the Machine Structure draws and approximation of the Machine Structure draws: Over the Machine Structure draws and approximation of the Machine Structure draws: Over the Machine Structure draws and approximation of the Machine Structure draws: Over the Machine Structure draws and approximation of the Machine Structure draws and approximation and application of the Machine Structure draws and application of the Machine Structure		
		Cancel	ок

----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 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 left 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

Details	
URN d- d	4
Region	
Identity Source	Management Authentication Session Settings Access Control Attributes
Identity Source	IAM Identity Center Change to external identity provider ⑦ You will manage all users and groups in IAM Identity Center. Users log in through the IAM Identity Center user po
Authentication Method	Password
Provisioning Method	Direct
Identity Store ID	d-9fbb718cd4
User Portal URL	Default URL: https://idcei 718cd4/portal
	Custom URL
	https://idcencom/a-123456/portal

4.3 Configuring an External Identity Provider

4.3.1 Overview

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 Editing SAML 2.0 Configuration

After the identity source is changed to an external identity provider, you can modify SAML 2.0 configurations as needed.

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** Choose **Settings** in the left 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 **Managing Certificates**.

Figure 4-7 Editing SAML 2.0 configuration

<	Manage SAML 2.0 Authe					
	1AM Identity Center works as a SAML 2.0 compliant service	e provider to your external identity provider. The I	following information displays metadata used to form the SAML trust n	elationship with your identity provider.		×
	Service Provider Details	LDownload Metadata File				
	IAM Identity Center User Portal URL	https://idcer	diportal 🗇			
	IAM Identity Center Assertion Consumer Service (ACS) URL	https://cn-m	/platform/samilacs/8d 71b28165f52			
	IAM Identity Center Issuer URL	https://cn-m	ittorm/saml/d-365d56b2df			
	Identity Provider Details					Edit
	Identity Provider Login URL https://auth	edirect				
	Identity Provider Issuer URL https://auth					
	Identity Provider Certificates					
	Import Delete					С
	Certificate Name			Created	Expires	
	OU: ager 1450 hul-sp, O+keymanage	r		Dec 21, 2015 14:40:54 GMT+08:00	Dec 18, 2025 14:40:54 GMT+08:00	
	OU= ger 1450 ui-sp. O=keymanage	и		Dec 21, 2015 14:40:54 GMT+08:00	Dec 18, 2025 14:40:54 GMT+08:00	

----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 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 left navigation pane.
- Step 4 On the Identity Source tab, select SCIM automatic provisioning for Provisioning Method and click Save.

5	
Settings (?)	
Details	
URN d- d	4
Region	
Identity Source	Management Session Settings Access Control Attributes
Identity Source	External identity provider Change to IAM identity Center 🕥 You will manage all users and groups in an external identity provider. Users log in on your identity provider page and are redirected to the IAM Identity Center user portal. After users log in to the Huawei Cloud access portal, they can access the Huawei Cloud accounts assigned to them.
Authentication Method	SAML.20 Modify SAML.20 Configuration
Provisioning Method	SCIM automatic previsioning Manual provisioning
Identity Store ID	d- d4
User Portal URL	Default URL: https://dcenter //18cd4.jportal
	O Custom URL
	https://doent // Enter a subdomain. portal
Save	

Figure 4-8 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**.

Х

Figure 4-9 Inbound automatic provisioning

	Automatic provisioning was successfully ena Next you will need to provide the following inform the trust relationship.	abled in IAM Identity Center. nation to configure your external provider and create	е
	ad or copy the access token as this is the only tin nerate new tokens at any time.	me it will be shown. It cannot be recovered later. How	weve
SCIM E	Endpoint		
_	Endpoint ps://sci	35a/scim/v2/	
Access	ps://sci i token JraWQiOiJmZUV4U0oxRVppelJZM21FY2E1cHJY	YaWJRYXJ4cjEzMzIkOGVSWFNwRWhyQyIsImFsZ	
Access D ey, 2liwidH	ps://sci		Njb38
Access Cess 2liwidH m9wZV CwiZXh	ps://sci i token JraWQiOiJmZUV4U0oxRVppelJZM21FY2E1cHJ IlwljoiSldUIn0.eyJzdW V5pZCJdLCJpc3MiOi hwljoxNzI0OTEzMTkx	YaWJRYXJ4cjEzMzlkOGVSWFNwRWhyQyIsImFsZ /yX25hbWUiOm51bGwsInl WIjbG91ZC5jb20iLCJhbGI 0ljoxNjkzMzc3MTkxLCJqd	Njb3l Ihcyl6 IGki0
Access Ceyson 2liwidH m9wZV CwiZXP bnRfY3 gMz5C dZGrYP	ps://sci stoken JraWQiOiJmZUV4U0oxRVppelJZM21FY2E1cHJY IlwljoiSldUIn0.eyJzdW N5pZCJdLCJpc3MiOi hwljoxNzI0OTEzMTkx BJIZGVudGlhbHM2N2 OtCPTzyvSyPa10qJtEcA9n7_y1HZGCaO_BaDB KdUPI9YuzGSHhuUg-	YaWJRYXJ4cjEzMzlkOGVSWFNwRWhyQyIsImFsZ /yX25hbWUiOm51bGwsInl WljbG91ZC5jb20iLCJhbGl	Njb38 Ihcyl6 IGki0 2Ulyj nfsufl

Step 6 Click Close.

----End

Disabling Automatic Provisioning

- **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** Choose **Settings** in the left navigation pane.
- Step 4 On the Identity Source tab, select Set Automatic Provisioning for Provisioning Method.

Settings 🕜	
Details	
URN d- d	
Region	
Identity Source	Management Session Settings Access Control Attributes
Identity Source	External identity provider Change to VM Identity Center 🕥
Authentication Method	SAML 2.0 Modily SAML 2.0 Configuration
Provisioning Method	SCIM automatic provisioning Manual provisioning Set Automatic Provisioning
Identity Store ID	d- d4
User Portal URL	Default URL: https://doiente 18co4/portal
	O Custom URL
	https://dcenter.it.com/ Enter a subdomain. /portal
Save	

Figure 4-10 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.

< Set Automatic Provisioning				
Automatic provisioning relies on the System for Cross-domain identity Management (SCIM) protocol to provision users fit	om your identity provider, and it requires that your identity provider supports compatible SC	2IM profile.		×
Configuration SCM Endport Interfacem Sc1-202054260514ccmv2/ 0 ⁴	X Disable Automatic Provisioning If you disable automatic provisioning user updates that are made in the identity provider will not be productorized. In addition, all access tokens will be removed			
Status Enabled Dirable	To re-enable automatic provisioning, you must generate a new access token. To confirm disablement, enter "DISABLE" below.			
Access Tokens	DISABLE			
Oenerate Delicite	OK Cancel			С
Access Token ID			Expires	
0 874i -ftce965cc45f	Active Jan	19, 2024 15:45:04 GMT+08:00	Jan 18, 2025 15:45:04 GMT+08:00	

Figure 4-11 Disabling automatic provisioning

----End

Generating or Deleting an Access Token

- **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** Choose **Settings** in the left navigation pane.
- **Step 4** On the **Identity Source** tab, select **Set Automatic Provisioning** for **Provisioning Method**.

IAM Identity Center	Settings 💿
Dashboard	Debils
Users	URN 4-3 2df
Groups Settings	Region
Multi-Account Permissions	Identity Source Management
	Identity Source External identity provider Change in VAM Identity Center 💿 You will manage all users and groups in an external identity provider: Users log in on your identity provider page and are redirected to the VAM Identity Center user portal. After users log in to the Huawer Cloud access portal, they can access the Huawer Cloud acce
	Authentication Method SAMI, 2.0 Modify SAMI, 2.0 Configuration
	Provisioning Method SOM automatic provisioning Manual provisioning Set Automatic Provisioning
	Identity Store ID 6-12df
	User Pontal URL https://do.e //fac4dipontal
	Sare

Figure 4-12 Setting automatic provisioning



Figure 4-13 Generating an access token

V Set Automatic Provisioning			
Automatic provisioning relies on the System for Cross-domain Identity Management (SCIM) protocol to provision	Generate Access Token	C SCIM profile.	х
Configuration SCIM Endpoint https://scim. 34685ebcm/v/2 C	Copy your new access token as this is the only chance you can do it. This access token cannot be recovered later. However, you can generate new tokens at any time.		
Status 🌒 Enabled Disable	Access token		
Access Tokens General Device Device	mt 7200km/ku1/9scn/ko12LC/1/2V/22bit/VU0051K0/sisn/ku28lpmmk/2 Wsp2Cu61_cb/s001/ode#krczur2/gzf2Miv/28tmy/s019/s04/fr22VI/06 12C5b20LC/htdliney/6bn/ks2cwl27tmi[onk]t00TErt/T01LCap2GWa9DW2E d69/2Vag2Cbbn/sacCwa9TF9[onk]ku2cwl710LCap2GWa9DW2E d69/2Vag2Cbbn/sacCwa9TF9[onk]ku2cwl710LCap2GWa9DW2E d69/2Vag2Cbbn/sacCwa9TF9[onk]ku2cwl710LCap2GWa9DW2E d69/2Vag2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V3p2Cbbn/sacCwa9TF9[onk]ku26cwl721LCap2GWa9DW2E d69/2V40mm4000000000000000000000000000000000		C
Access Token ID	Ay_z9puLH50_T2rFZEbl6k4Sg9573-kN7uniPIZu_dv3Tu7aDy0KhktfBDscwNeWG LnmCwPOd6gzfPcefyMHaorkQhtRLX8nh8JjuH7HJENeIjTD3UY9wi04bwNuBGN	d	Expires
b31b2al Dofe3ad449	jeloG7NEd232_J4cppJrgQA1qx/WbTcx8XSV-PcrhPgFIDZKmtreU5NectVd8Ot7yG Q4QGTSy5BZCOrFKAqfDqzMJkQXS_06QAw	, 2023 14:33:11 GMT+08:00	Aug 29, 2024 14:33:11 GMT+08:00
Sriufse: 1920072878	Close	, 2023 14:39:05 GMT+08:00	Aug 29, 2024 14:39:05 GMT+08:00

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 4-14 Deleting an access token

< Set Automatic Provisioning								
Automatic provisioning telles on the System for Cross-domain Identity Management (SCIM) protocol to provision users from your identity provider, and I requires that your identity provider supports compatible SCIM profile.								
Configuration	Delete Access Token	×						
SCIM Endpoint https://scim/v2/ 🖒 Status @ Enabled Disable	Any inbound automatic provisioning operations using this token will no longer authorized. This operation is irreversible. Delete the token?	e e						
	Deletion cannot be undone. To confirm deletion, enter "DELETE" below. DELETE							
Access Tokens Generate Delete	OK			С				
Access Token ID	olaius	Created	Expires					
76888 Jeac36983a	Active	Sep 22, 2023 17:01:07 GMT+08:00	Sep 21, 2024 17:01:07 GMT+08:00					

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 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 left 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**.

Settings (?)									
Details	Details								
URN d- 14	м								
Region									
Identity Source Management Session Settings Access Control Attributes									
Identity Source	External identity provider Change to VMI identity Center 🕥								
Authentication Method	SAMIL20 Modify SAMIL2.0 Configuration								
Provisioning Method	SCIM automatic provisioning Manual provisioning Sel Automatic Provisioning								
Identity Store ID	d- d4								
User Portal URL	Default URL: https://idcent 37f8cc44portal								
	O Custom URL								
	https://dcencom/_Enter a subdomainportal								
Save									

Figure 4-15 Enabling manual provisioning

----End

4.3.5 Managing 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. The certificate is usually included in the IdP SAML metadata file and automatically installed during the metadata file upload.

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. All imported certificates are automatically active. A maximum of two certificates are supported. 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

As a security best practice, upon any signs of compromise or mishandling of an existing SAML certificate, you should immediately remove and rotate that certificate.

Rotating a Certificate

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 console.
 - 2. Click in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.
 - 3. Choose **Settings** in the left 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 4-16 Importing a certificate

<	Manage SAML 2.0 Authe						
	WM Kenthy Center works as a SAML 2.8 compliant services provider to your external identity provider. The following intermation displays metabatia used to form the SAML thus relatenting with your identity provider.						
	Service Provider Details						
	IAM Identity Center User Portal URL IAM Identity Center Assertion Consumer Service (ACS) URL	Import SAML 2.0 Certificate	0				
	IAM Identity Center Issuer URL	You might need to rotate your x509 certificates, either for fault tolerance purposes or due to compliance requirements. Rotating a certificate involves importing a certificate and then deleting the old one.	0				
	Identity Provider Details	The certificate file must be in PEM encoding format.				Edit	
	Identity Provider Login URL https://ex. om/s Identity Provider Issuer URL https://ex. om/-	Certificate File Select File					
	Identity Provider Certificates	Import Certificate Cancel					
	Import Delete					C	
	Certificate Name			Created	Expires		
	OU+iam-authui-sp, O=keymanager 1450680054939 OU=iam-authui-sp, O=keymanager			Dec 21, 2015 14:40:54 GMT+08:00	Dec 18, 2025 14:40:54 GMT+08:00		

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 and click **Delete**.
- 2. In the displayed dialog box, enter **DELETE** and click **OK**.

Figure 4-17 Deleting a certificate

Manage SAML 2.0 Authe								
IAM Identity Center works as a SAML 2.0 compliant service provider to your external identity provider. The following information displays metadela used to form the SAML brust relationship with your identity of the same service provider.						dentity provider.		
Service Provider Details	Download Metadata File							
IAM Identity Center User Portal URL			×	Т				
IAM Identity Center Assertion Consumer Service (ACS) URL		2.0 Certificate tificate, ensure that your identity provider no longer uses IL responses. Delete this certificate?	his	201	b9 🗇			
IAM Identity Center Issuer URL								
	Subject Name	OU=i	n					
Identity Provider Details	Certificate Serial Number	145 39						
Identity Provider Login URL https://aut om/	Issuer Name	OU+iam-authui-sp, O+keymanager		1				
Identity Provider Issuer URL https://au :om/-	Created	Dec 21, 2015 14:40:54 GMT+08:00		1				
Identity Provider Certificates	Expires	Dec 18, 2025 14:40:54 GMT+08:00						
Import Delete	Deletion cannot be undone	To confirm deletion, enter "DELETE" below.		1				
Certificate Name	DELETE					Created	Expires	
OU=iam-authui-sp, O=keymanager 1450 739 OU=iam-authui-sp, O=keymanage		OK Canoel				Dec 21, 2015 14:40:54 GMT+08:00	Dec 18, 2025 14:40:54 GMT+08:00	
OU=lam-authul-sp, O=keymanager 145 339 OU=lam-authul-sp, O=keymanager				J		Dec 21, 2015 14:40:54 GMT+08:00	Dec 18, 2025 14:40:54 GMT+08:00	

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

----End

4.4 Supported Identity Providers

4.4.1 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.

4.4.2 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 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 left 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

Settings ⑦					
Details					
URN d- 4 Region	Delete IAM Identity Center Configuration?	×			
	This operation will delete IAM Identity Center instance "ins-049b88455c009275" an configuration data in the instance.	l all			
Identity Source Management Authentication	 Select all the check boxes to confirm that you want to delete all the configuration this IAM Identity Center instance. All users and groups in the IAM Identity Center will be deleted. 	data in			
Delegated Administrator ⑦	All user assignments to Huawei Cloud accounts will be deleted.	ок 🗹			
Register	All permission sets of Huawei Cloud accounts will be deleted.	🗹 ок		Enter an account name. Q	2
Account Name	2. To confirm deletion, enter "ins-0f9b68455c009275" below. ins-0f9b68455c009275		Delegation Time	Operation	
test10			Jan 17, 2024 16:42:17 GMT+08:00	Deregister	
	OK Cancel				
Delete IAM Identity Center Configuration					
This operation will delete all data in the IAM Identity Center config	guration, including user assignments and permission sets you configured for Huawel Cl	ud accounts. I	f you are using IAM Identity Center as your identity sourc	e, this operation will also delete all users and groups from IAM Identity	
Center. You can delete this configuration if you need to create a r	new configuration from scratch or enable IAM Identity Center in a different region.				
Delete					

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:

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.

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

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 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 left 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.

Step 6 Click Save.

----End

6.2.2 Choosing an MFA Device Type

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

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** Choose **Settings** in the left 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
- 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 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 left 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.

Step 6 Click Save.

----End

6.2.4 Allows Users to Binding Their Own MFA Devices

You can enable users to bind their own MFA devices.

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** Choose **Settings** in the left 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.
- 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 **Allows Users to Binding Their Own MFA Devices**.

Binding an MFA Device

- 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** In the user list, click a username to go to the user details page.

Figure 6-1 Selecting a user

Users ⑦							Create User
Delete					Q Enter a username.		C
Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
Chen	S Enabled	chen	May 12, 2023 09:56:56 GMT+08:00	May 12, 2023 09:56:56 GMT+08:00	Manual	Manual	Delete
33@3.com	S Enabled	33@3.com	Oct 26, 2023 11:16:23 GMT+08:00	Oct 26, 2023 17:02:05 GMT+08:00	Manual	Manual	Delete
. 111	Enabled	111	Dec 08, 2023 09:33:02 GMT+08:00	Dec 08, 2023 09:33:02 GMT+08:00	Manual	Manual	Delete

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

Figure 6-2 Binding an MFA device

Groups MFA Devices Active Session	IS		
Bind MFA Device			Q Enter a device name.
Device Name	Туре	Created	Operation

- **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.

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 device on 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 select both the authenticator App and security key, users logging in to the user portal will be authenticated using the security key first and then the authenticator App later.

----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 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 6-3 Selecting a user

Username Status Display Name Created Updated Creates Mode Update Mode Operational thm Image: Created Advance Mary 12, 2023 09:55:50 OMT-08:00 Mary 12, 2023 09:55:50 OMT-08:00 Manual Manual Deleter 130(0.1cm Image: Created 33(0.3 cm Oct 26, 2023 11:16:23 OMT-08:00 Cct 26, 2023 17:02:05 GMT-08:00 Manual Manual Deleter	rs (?)							Create User
Chem © Enabled chem May 12, 2023 09:56 56 GMT+08:00 May 12, 2023 09:56 56 GMT+08:00 Manual Manual Detete 133@3.com © Enabled 33@3.com Cht 26, 2023 11:16 23 GMT+08:00 Cht 26, 2023 17:02:05 GMT+08:00 Manual Manual Detete	Delete					Q Enter a username.		C
33@3.com Oct 26, 2023 11:16:23 GMT-98:00 Oct 28, 2023 17:02:05 GMT-88:00 Manual Manual Debite	Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
	Chen	Enabled	chen	May 12, 2023 09:56:56 GMT+08:00	May 12, 2023 09:56:56 GMT+08:00	Manual	Manual	Delete
111 © Enabled 111 Dac 08 2023 09 33 02 GMT-08 00 Dac 08 2023 09 33 02 GMT-08 00 Manual Manual Delete	33@3.com	Enabled	33@3.com	Oct 26, 2023 11:16:23 GMT+08:00	Oct 26, 2023 17:02:05 GMT+08:00	Manual	Manual	Delete
	111	Enabled	111	Dec 08, 2023 09:33:02 GMT+08:00	Dec 08, 2023 09:33:02 GMT+08:00	Manual	Manual	Delete

- **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 6-4 Renaming an MFA device

Groups MFA Devices			
Bind MFA Device			Enter a device name. Q
Device Name	Туре	Created	Operation
manual_user_test'MFA1	Authenticator app	Aug 31, 2023 21:50:05 GMT+08:00	Rename Delete
manual_user_test'MFA2	Authenticator app	Aug 31, 2023 22:43:11 GMT+08:00	Rename Delete

----End

Deleting an MFA Device

- **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** In the user list, click a username to go to the user details page.

Figure 6-5 Selecting a user

Users ⑦							Create User
Delete					Q Enter a username.		C
Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
chen	C Enabled	chen	May 12, 2023 09:56:56 GMT+08:00	May 12, 2023 09:56:56 GMT+08:00	Manual	Manual	Delete
33@3.com	📀 Enabled	33@3.com	Oct 26, 2023 11:16:23 GMT+08:00	Oct 26, 2023 17:02:05 GMT+08:00	Manual	Manual	Delete
. 111	Enabled	111	Dec 08, 2023 09:33:02 GMT+08:00	Dec 08, 2023 09:33:02 GMT+08:00	Manual	Manual	Delete

- **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 6-6 Deleting an MFA device

Groups MFA Devices				
Bind MFA Device			Enter a device name.	QC
Device Name	Туре	Created	Operation	
manual_user_testMFA1	Authenticator app	Aug 31, 2023 21:50:05 GMT+08:00	Rename Delete	
manual_user_testMFA2	Authenticator app	Aug 31, 2023 22:43:11 GMT+08:00	Rename Delete	

----End

7 Permissions Management

7.1 Creating an IAM User and Granting Permission to Use IAM Identity Center

You can use **Identity and Access Management (IAM)** to implement fine-grained permissions control over your IAM Identity Center resources. 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 users only the permissions required to perform a given task based on their job responsibilities.
- Entrust an account or a cloud service to perform professional and efficient O&M on your IAM Identity Center resources.

If your account meets your permissions requirements, you can skip this section.

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

Prerequisites

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

Process Flow

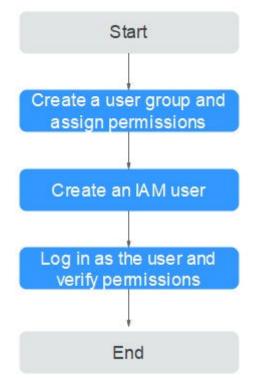


Figure 7-1 Process of granting IAM Identity Center permissions

- 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 permissions.

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": [
```



8 Auditing

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.

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	UpdateMfaDeviceMana- gementForldentityStore
Adding a user-defined domain name	Instance	CreateAlias
Enabling access control attributes for a specified instance	Instance	CreateInstanceAccess- ControlAttributeConfigu- ration
Disabling access control attributes for a specified instance	Instance	DeleteInstanceAccess- ControlAttributeConfigu- ration
Updating access control attributes for a specified instance	Instance	UpdateInstanceAccess- ControlAttributeConfigu- ration

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

Operation	Resource Type	Event Name
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
Attaching a custom policy to a permission set	PermissionSet	PutCustomPolicy

Operation	Resource Type	Event Name	
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	UpdateMfaDeviceForUs- er	
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	
Removing a user from a group	GroupMembership	DeleteGroupMembership	

Operation	Resource Type	Event Name	
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	BatchReplaceMember- ship	
Creating external identity provider configuration	IdP	CreateExternalIdPConfi- gurationForDirectory	
Enabling external identity provider	IdP	EnableExternalIdPConfi- gurationForDirectory	
Deleting external identity provider configuration	IdP	DeleteExternalIdPConfi- gurationForDirectory	
Disabling external identity provider	IdP	DisableExternalIdPConfi- gurationForDirectory	
Updating external identity provider configuration	IdP	UpdateExternalIdPConfi- gurationForDirectory	
Deleting a certificate	IdP	DeleteExternalIdPCertifi- cate	
Importing a certificate	IdP	ImportExternalIdPCertifi- cate	
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	

8.2 Querying Real-Time Traces

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 OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

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

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

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.
- 5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
 - Enter any keyword in the search box and click Q to filter desired traces.
 - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
 - Click $^{
 m C}$ to view the latest information about traces.
 - Click 🙆 to customize the information to be displayed in the trace list. If

Auto wrapping is enabled (**C**), 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: You can query traces generated during any time range in the last seven days.
- Click Export to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
- 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 5000 records.
 - Click $^{\mathbb{C}}$ to view the latest information about traces.
- 8. Click \checkmark on the left of a trace to expand its details.

Trace Name			Resource Type	Trace Source	Resource ID ⑦	Resource Name ⑦	Trace Status ⑦	Operator ⑦	Operation Time	Operation
crea	teDockerConfig		dockerlogincmd	SWR	-	dockerlogincmd	📀 normal		Nov 16, 2023 10:54:04 GMT+08:00	View Trace
equest										
race_id										
ode	200									
race_nan	ne create	DockerConfig								
esource_	type docke	rloginemd								
race_ratio	ng norma	normal								
ipi_versic	in									
nessage	create	createDockerConfig, Method: POST Uri=N2/Imanage/utils/secret, Reason:								
ource_ip										
lomain_ic										
race_type	e ApiCa									

9. Click **View Trace** in the **Operation** column. The trace details are displayed.

View Trace



- 10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
- 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. For details about the quota of IAM Identity Center, see **Notes and Constraints**.

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

How Do I Increase My Quota?

- 1. Log in to the management console.
- In the upper right corner of the page, choose Resources > My Quotas. The Quotas page is displayed.

Figure 9-1 My Quotas



- 3. Click Increase Quota.
- 4. On the Create Service Ticket page, set the parameters.

In the **Problem Description** area, enter the required quota and the reason for the quota adjustment.

5. Read the agreements and confirm that you agree to them, and then click **Submit**.

10 Change History

Released On	Change History
2024-02-20	This issue is the third official release.
	Modified the following content:
	Added Managing Permission Set Tags.
	 Updated Creating a Permission Set and Viewing or Modifying a Permission Set.
	Added Attribute-based Access Control (ABAC).
2023-11-24	This issue is the second official release.
	Modified the following content:
	Added optional user details in Creating Users.
	 Added Configuring the Duration of the User Portal Session.
	 Added an MFA device type security key in MFA Management.
2023-08-30	This issue is the first official release.