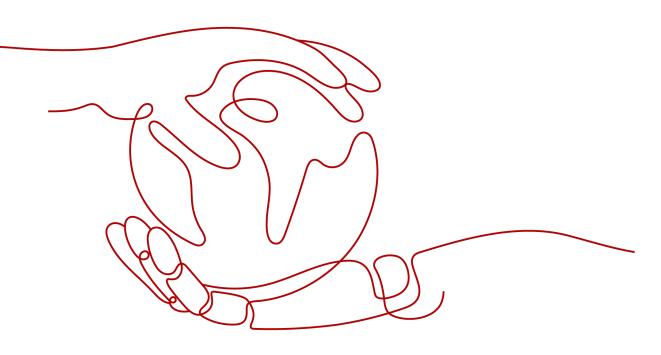
IAM Identity Center

Getting Started

 Issue
 01

 Date
 2023-08-30





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

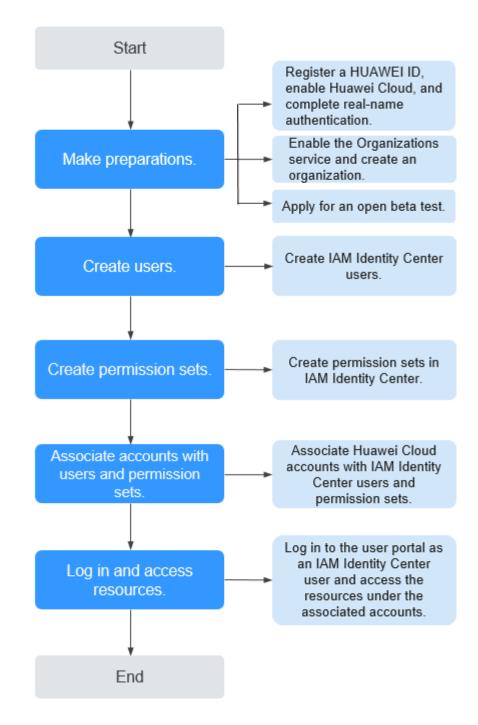
1 Overview	1
2 Making Preparations	3
3 Creating Users and Permission Sets	5
4 Associating Accounts with Users and Permission Sets	12
5 Logging In as an IAM Identity Center User and Accessing Resources	16



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

The following figure shows how to use IAM Identity Center.

Figure 1-1 Flowchart



2 Making Preparations

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

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

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

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

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

For details, see **Registering a HUAWEI ID and Enabling Huawei Cloud** Services.

4. Complete real-name authentication by following the instructions in **Real-Name Authentication Overview**.

NOTE

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

Enabling the Organizations Service and Creating an Organization

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

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

- **Step 1** Go to the **Enterprise Center** console.
- Step 2 Click Enable for Free.

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

- **Step 3** Select I have read and agree to the HUAWEI CLOUD Enterprise Management Service Agreement and click Enable for Free. Your account will become an enterprise master account. For details, see Enabling Enterprise Center.
- **Step 4** Go to the Organizations console.
- **Step 5** Click **Enable Organizations** to enable the Organizations service.
- **Step 6** After the Organizations service is enabled, your organization and the root are automatically created, and your login account is defined as the management account. For details, see **Creating an Organization**.
- **Step 7** Invite an account to join your organization. For details, see **Inviting an Account to Join Your Organization**.

----End

Applying for an Open Beta Test and Enabling IAM Identity Center

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

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

The review result will be sent to you via email and SMS message within five working days.

- 6. Choose **Resources** > **Open Beta Tests** in the menu bar to view your application status.
- 7. After your application is approved, click **Enable Now** on the **IAM Identity Center** page to enable the service.

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

3 Creating Users and Permission Sets

Creating Users

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

- **Step 1** Log in to the **Huawei Cloud console**.
- Step 2 Click in the upper left corner of the page and choose Management & Governance > IAM Identity Center.
- **Step 3** In the navigation pane, choose **Users**.
- Step 4 Click Create User in the upper right corner of the page.

Figure 3-1 Creating users

IAM Identity Center	Users ⑦							Create User
Dashboard Users	Delete					Q Enter a username.		C
Groups	Username	Status	Display Name	Created	Updated	Creation Mode	Update Mode	Operation
Settings	chen	C Enabled	chen	May 12, 2023 09:55:56 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	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 are mandatory. The contact methods, job-related information, and address are optional and can be set as needed.

Figure 3-2 Configuring basic information

< Create User			
1 Set User Details			
User Details			
* Username	Enter a username.	* Family Name	Enter a family name.
* Given Name	Enter a given name.	* Display Name	This is hysically the full name of the workforce user. Enter a display name.
* Email Address	This email address will be used to receive password setup or reset instructions. email@example.com	Confirm Email * Address	emal@example.com
* Password	Send an email to this user with password setup instructions. Cenerate a one-time password that you can share with this user.		
✓ Contact Method	s - Optional		
✓ Job-related info	rmation - Optional		
✓ Address - Optio	nai		
			Cancel Next

Table 3-1 User details

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

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

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

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

	Enter a group name.	Q C Create Group		Enter a name.
iroup Name	Description	Group Name	Description	Operation
2 00	-	123	-	Ranove

- **Step 7** In the **Confirm** step, confirm the configuration and click **OK** in the lower right corner of the page. The IAM Identity Center user is created and displayed in the user list.
 - If **Send an email to this user with password setup instructions.** is selected for **Password** in step **Step 5**, the user list will be displayed, showing the newly created IAM Identity Center user.
 - If Generate a one-time password that you can share with this user. is selected for Password in step Step 5, a page that contains detailed information about the one-time password will be displayed. You can copy the information and send it to the user. The user can use the username and one-time password to log in through the user portal URL.

Figure 3-4 Confirming user creation

Create User			
et User Ortalis (2) (Optional) Add User to Groups 🔕 Continn			
ser Details			
isername 21 Family Name 2			
New Name n Display Name 12			
mail Adoress com			
/ Contact Methods - Optional			
Job-related information - Optional			
Address - Optional			
roups			
Group Name Description			
letshipopu –			
	Cancel	Previous	ок

----End

Creating a Permission Set

A permission set defines a collection of one or more IAM policies and controls the permissions of IAM Identity Center users to access resources. Creating permission sets is mandatory. When logging in to the management console as an IAM Identity Center user to access resources of multiple accounts, you must associate the user with permission sets. Otherwise, the user cannot access any resources after login.

- **Step 1** Log in to the **Huawei Cloud console**.
- Step 2 Click in the upper left corner of the page and choose Management & Governance > IAM Identity Center.
- **Step 3** In the navigation pane, choose **Multi-Account Permissions > Permission Sets**.
- **Step 4** Click **Create Permission Set** in the upper right corner of the page.

Figure 3-5 Creating a permission set

IAM Identity Center	Permission Sets ③					Create Permission Set
Dashboard					Permission • Enter a permission set name.	Q C
Users	Permission Set Name	Description	URN	Attachment Status	Created	Operation
iroups	testSTS404		IdentityCenter::c086cf249ced4bf2b811d70c3932f84f;permissionSet1.	. O Attached	Jul 27, 2023 20:44:52 GMT+08:00	Delete
Settings Julti-Account	testSKConflict	-	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84fpermissionSet1.	. O Attached	Jul 27, 2023 20:51:58 GMT+08:00	Delete
Permissions *	test	-	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84fpermissionSet i	O Attached	Jul 31, 2023 11:50:07 GMT+08:00	Delete
Permission Sets	fafaagfargarg	-	IdentityCenter::c086cf249ced4bf2b81fd70c3932f84f.permissionSet1.	 Not attached 	Jul 31, 2023 17:19:28 GMT+08:00	Delete
Accounts	Jact 1	_	IdentityCenter-c098-f249ced4bf2b916470c2932994f.nemizsionSet i	O Not attached	Aug 17, 2023 15:25:23 GMT+09:00	Dalata

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

Figure 3-6 Setting permission set details

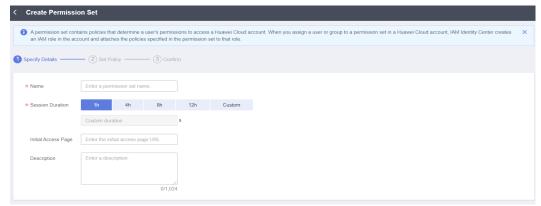


 Table 3-2 Permission set details

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 3-7 Setting policies

	Create Permis	ision Set							
		contains policies that determine a user's permissions to acce in the permission set to that role.	ss a Huawei Cloud accour	nt. When you assign a user or group to a permission set in	a Huawei Cloud account, IAM Identity Cent	ler creates an IAM i	role in the acco	unt and attaches th	e X
0	Specify Details —	2 Set Policy 3 Confirm							
	Identity Policy	Identity policies can be customized and give you more gran	ular, more flexible control	of your resources.					
	 System-defined IAM provides system View Selecter 	stem-defined policies that define the common actions of clou	d services. You can directl	ly choose from these IAM system-defined policies, but carr		Enter a policy nam	ie or descriptio	n. C	C
	V F	Policy Name	Туре	Description					
	v 🗹 \	VPCEPFullAccessPolicy	Identity policy	All permissions of VPCEP Service.					
	v 🔽 \	VPCReadOnlyPolicy	Identity policy	The read-only permissions to all VPC resources.					
	Custom identity (Custom identity (Policy View Policy Content	coloies can be created to supplement system-defined identit Visual editor JSON	y policies for fine-grained p	permissions control	C (Optional) Select resource	C (Octional)	Add request c	andtion 🕀	Ū
		Alow Deny				((),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
							Cancel	Previous	Next

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

Figure 3-8 Confirming configurations

< Create Permission Set			
A permission set contains policies that determine a user's permission policies specified in the permission set to that role.	ions to access a Huawei Clo	ut account. When you assign a user or group to a permission set in a Hauve Cloud account, WAI Konthy Center creates an WAI role in the account and attaches the	X
Specify Details Set Policy Confin	n		
Specify Details			
Name 123			
Session Duration 1h			
Initial Access Page			
Description			
System-defined policies			
Policy Name	Туре	Description	
VPCEPFullAccessPolicy	Identity policy	All permissions of VPCEP Service.	
V VPCReadOnlyPolicy	Identity policy	The read-only permissions to all VPC resources.	
		Cancel Previous	ОК

NOTE

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

----End

4 Associating Accounts with Users and Permission Sets

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

Procedure

- Step 1 Log in to the Huawei Cloud console.
- Step 2 Click in the upper left corner of the page and choose Management & Governance > IAM Identity Center.
- **Step 3** In the navigation pane, choose **Multi-Account Permissions** > **Accounts**.

By default, accounts are displayed in an organizational hierarchy structure. You

can click 📃 to switch to the list view.

Figure 4-1 Account view

Accounts 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 4-2 Selecting accounts

counts ⑦				
The following accounts have been configured and can be managed in Huavel 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**.

Figure 4-3 Assigning users/groups

User	Q. Enter a username. C Create User			Q Enter a name.
Туре	Status	Username	Туре	Operation
User	Enabled	chen chen	User	Remove
User	Enabled	33@3.com 33@3.com	User	Remove
User	Enabled			
	Type User User	Tryse Status Uzer © Ehabled Uzer © Enabled	Type States Username User © Ensitied chm User © Ensitied 33(g) com Jags com 33(g) com	Type Status Userante Type User © Exelid dan User User © Exelid 33§3 com User

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

Figure 4-4 Selecting one or more permission sets

lect one or more permission	sets.					
	Permission Enter a permission set name. Q	Create Permission Set			Enter a name.	a
olicy Name	URN		Policy Name	URN		Operation
est	IdentityCenter:	tpermissionSet ins-4d2	test 	Identity Center	permissionSet	Remove
esteee	IdentityCenter:	t permissionSet ins-4d2	testeee	IdentityCenter	permissionSet	Remove
wanghangtest	IdentityCenter:	t permissionSet 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				
factmanul lear						

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

Figure 4-5 Confirming configurations

ect User/Group —— (2) Select Permis	ision Set (3) Confirm				
ers/Groups					
sername		Type			
st111		User			
st222		User			
rmission Sets					
olicy Name	Description	URN		Created	
st	-	Identity Center	permissionSet:ins-4d2b8	Sep 07, 2023 16:32:26 GMT+08:00	
steee	-	Identity Center	permissionSet:ins-4d2b8	Sep 07, 2023 16:49:36 GMT+08:00	

----End

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

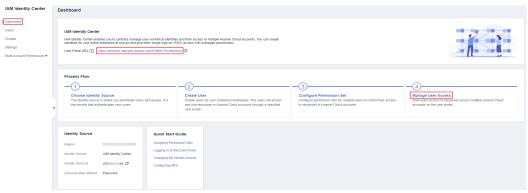
After associating member accounts of an organization with an IAM Identity Center user and permission sets, you can use the IAM Identity Center username and password to log in to the console through the user portal URL and access resources according to the permissions included in the associated permission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

Procedure

- Step 1 Log in to the Huawei Cloud console.
- **Step 2** Click = in the upper left corner of the page and choose **Management & Governance** > **IAM Identity Center**.
- **Step 3** In the navigation pane, choose **Dashboard**. On the displayed page, obtain the user portal URL.

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

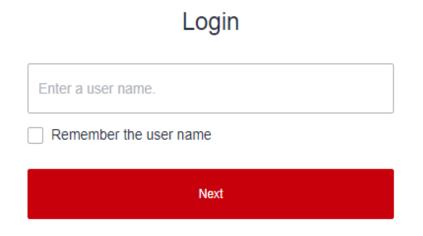
Figure 5-1 User portal URL



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

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

Figure 5-2 Login



- **Step 5** Enter the password, and click **Log In**.
- **Step 6** Under a specific account, locate your desired permission set and click **Access Console** in the **Operation** column to access resources according to the permissions included in the permission set.

Figure 5-3 Accessing resources

✿ qii →st 		V
Pe n Set	Description	Operation
te: I	-	Access Console
te: Vict		Access Console
ter		Access Console

----End