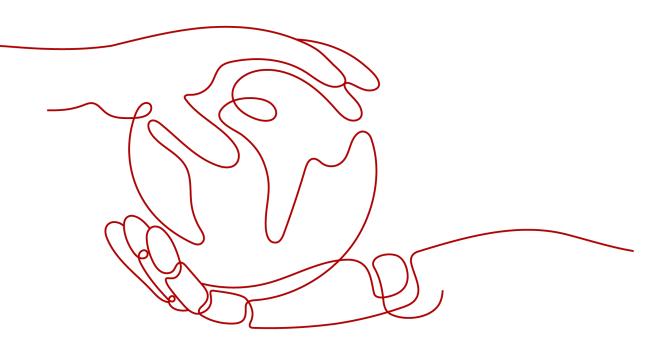
Identity and Access Management

Getting Started

 Issue
 09

 Date
 2025-04-28





Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions

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

Notice

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

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

Contents

1 Creating a User Group and Assigning Permissions	.1
2 Creating an IAM User and Logging In	7

Creating a User Group and Assigning Permissions

Scenarios

If you do not want to create an account for every person in your enterprise, you can use Identity and Access Management (IAM). Only the enterprise's administrator needs to create an account. The account can be used to create user groups and assign permissions. Then, the IAM users created for the enterprise personnel can be added to different user groups based on their job responsibilities. For the definitions of an account and IAM user, see **Basic Concepts**.

The following shows how an enterprise administrator uses IAM to create user groups and assign permissions.

Procedure

Step	Description
Preparations	Sign up for a HUAWEI ID and complete real- name authentication.
Step 1: Create a User Group	Create a user group, which is the minimum authorization unit.
Step 2: Assign Permissions to the User Group	Assign permissions defined by roles or policies to the user group. Users added to this group can inherit the assigned permissions from it.

Preparations

If you already have an account, go to **Step 1: Create a User Group**. If you do not have an account, perform the following operations to create one:

- 1. Visit https://www.huaweicloud.com/intl/en-us/ and click Sign Up.
- 2. Sign up for a HUAWEI ID and enable Huawei Cloud services.

After the HUAWEI ID is created, the system redirects you to your personal information page.

3. INOTE

IAM is a free service. You do not need to pay for it.

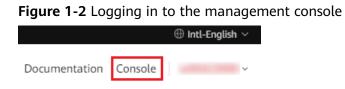
Step 1: Create a User Group

Step 1 Log in to Huawei Cloud using your account.

Figure 1-1 Logging in to Huawei Cloud

	HUAWEI ID login	
Phone/Email/Lo	igin ID/HUAWEI CLOUD account name	
Password		Ø
	LOG IN	
	Register Forgot password?	
	Use Another Account	
	d network information will be used to help ence. Learn more	improve

Step 2 Access the Huawei Cloud management console.



Step 3 On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.

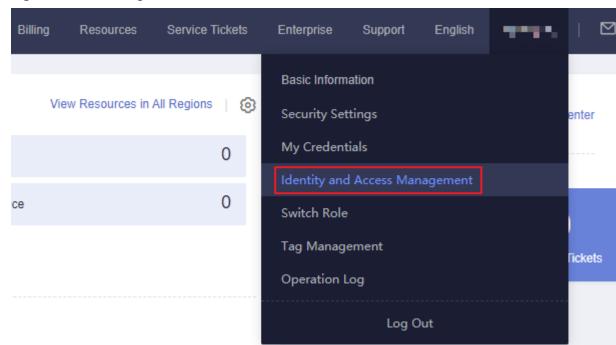


Figure 1-3 Accessing the IAM console

Step 4 On the IAM console, choose User Groups and click Create User Group.

Figure 1-4 Creating a user group

IAM	User Groups 💿 Create User Group
Users	
User Groups	Delete User groups available for creation: 12
Permissions ~	Q Enter a group name.
Projects	Name ⊕ Users Description ⊕ Created ⊕ Operation
Agencies	developers 0 Jul 03, 2024 16.34.07 GM Authorize Modify Manage User Delete

Step 5 In the displayed dialog box, enter a name for the developer user group.

Only letters (case-sensitive), digits, spaces, hyphens (-), and underscores (_) are allowed.

Figure 1-5 Setting user group details

User Groups / Create L	lser Group	
★ Name	Developer	
Description	Enter a brief description.	
	OK Cancel	0/255 1/2

Step 6 Click **OK** to create a developer user group.

You will be redirected to the user group list and the created developer user group is displayed in the list.

----End

Step 2: Assign Permissions to the User Group

Assume that developers in the enterprise need to use ECS and OBS, so the administrator needs to perform the following operations to assign the required permissions to the developer user group to enable access to these services. For details about the permissions of all cloud services, see **System-defined Permissions**.

Step 1 Determine the permissions required by the users in the user group.

Table 1-1 lists the required permissions. You can determine which permissions are required by referring to **System-defined Permissions**. The application scope is determined by geographic areas where services are deployed.

- Region-specific project-level services: If permissions are assigned for a regionspecific project, the permissions are only applied in that project. For example, if you assign permissions only for **CN-Hong Kong**, IAM users have no permissions to access resources in other projects.
- Global services: Global services are deployed in all regions. You do not need to switch regions when accessing global services. For example, if you grant OBS permissions to an IAM user, the user can access OBS resources in all regionspecific projects.

Cloud Service	Application Scope	Permissions
ECS	Region-specific projects	ECS FullAccess
OBS	Global regions	OBS OperateAccess

Table 1-1 Required permissions

Step 2 In the user group list, click **Authorize** in the row containing the developer user group.

Figure 1-6 Authorizing a user group

Identity and Access Management	User Groups 💿	p
Users	Delete User groups available for creation: 17	
User Groups		
Permissions 🗸	Q Enter a group name.	
Projects	Name ⊕ Users Description ⊕ Created ⊕ Operation	
Agencies	Developer 0 Oct 08, 2024 16:18:22 Authorize Modify Manage User Delete	

Step 3 Assign permissions to the user group for region-specific projects.

1. As shown in **Table 1-1**, ECS is a region-specific project-level service. Select desired permissions for the project-level service and click **Next**.

Figure 1-7 Selecting required permissions

< Authorize User Group	
Select PolicyRole 2 Select Scope 3 Firsth	
Assign selected permissions to Developer.	Create Policy
View Selected (1) Copy Permissions from Another Project	All policie v All services v Fuzzy se v Enter a policy name Q
Policy/Role Name	Туре
ECS FullAccess All permissions of ECS service.	System-defined policy
	Cancel

2. Select **Region-specific projects** for **Scope**, select **CN-Hong Kong**, and click **OK**.

Then users in the developer user group can only access resources in **CN-Hong Kong**.

Figure 1-8 Specifying the permission scope

Authorize User Group		
Select Policy/Role 2 Select Scope 3 Fine		
The following are recommended scopes for the permissions you selected. Set	elect the desired scope requiring minimum authorization.	×
Scope		
All resources		
Region-specific projects IAM users will be able to use resources in the selected region-specific projects The selected permissions will be applied to resources in the region-specific projects		
Total projects: 13. Select the desired projects.		Enter a project name or description. Q
Project [Region] \ominus	Description	
af-south-1 [AF-Johannesburg]		
ap-southeast-1 [CN-Hong Kong]	-	
ap-southeast-3 [AP-Singapore]		
ap-southeast-4 [AP-Jakarta]		
cn-east-2 [CN East-Shanghai2]		
cn-east-3 [CN East-Shanghai1]	-	
		Previous

Step 4 In the user group list, click **Authorize** in the row containing the developer user group.

Figure 1-9 Authorizing a user group

User Groups ③			Create User Group
Delete User groups available for creation: 17			
Q Enter a group name.			
Name 🔶	Users Description 🕀	Created \ominus	Operation
Developer	0	Oct 08, 2024 16:18:22 GMT	Authorize Modify Manage User Delete

Step 5 Assign permissions to the user group for global services.

1. Select **OBS OperateAccess** and click **Next**.

Cancel

Authori	ze User Group						
1 Select	Policy/Role 2 se	elect Scope (
-							
ssign sele	cted permissions to Develope	er.					Create Pol
View S	elected (1) Copy Permissions Project	s from Another All policie	es/roles ~	All services	✓ Fuzzy sea ✓	Enter a policy name, role name, or o	lescriptior Q
	Policy/Role Name				Туре		
	OBS OperateAccess Basic operation permissions to				System-defined policy		

Figure 1-10 Selecting OBS OperateAccess

2. Select **Global services** for **Scope** and click **OK**.

Figure 1-11 Specifying the permission scope

< Authorize User Group	
Steled PakyRole 3 Select Scope 3 Front	
The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.	×
Scope	
All resources	
Constraints Constrain	
	Previous

After the permissions are assigned, click the name of the developer user group to view the assigned permissions on the **Permissions** tab of the user details page.

NOTE

OBS permissions will be applied about 15 to 30 minutes after the authorization is complete.

----End

2 Creating an IAM User and Logging In

Scenarios

The account created in the previous section can be used to create an IAM user and add the IAM user to the developer user group. The IAM user has their own username and password. They can log in to Huawei Cloud and use resources based on assigned permissions.

Procedure

Step	Description
Step 1: Create an IAM User	Create an IAM user and add it to the user group to obtain permissions.
Step 2: Log In to the Console as an IAM User	Log in to the management console as an IAM user and use resources within the permissions scope.

Step 1: Create an IAM User

Step 1 Choose **Users** from the navigation pane, and click **Create User**.

Set mandatory IAM user parameters by referring to the following table. Retain the default settings for other parameters.

- **Step 2** Specify the user details and access type.
 - 1. Enter a username.

Figure 2-1 Setting user details

Users / Create User						
1) Set User Details —				al) Add User to Group		
* User Details	The username, email address	s, and mobile number can be used a	s login credentials.			
	* Username	Email Address	Mobile Number	Description	External Identity ID	Operation
	James	Enter an email address.	+86 (Chinese • Enter	r a mobile number. Enter a brief description.	Enter an external identity	Delete

NOTE

IAM users can log in to Huawei Cloud using their usernames, email addresses, or mobile numbers.

Table 2-1 User details

Parameter	Exampl e	Description
Username	Alice	(Mandatory) Username used by an IAM user to log in to Huawei Cloud.
		Use only letters, digits, spaces, hyphens (-), underscores (_), and periods (.). Do not start with a digit or space.
Email Address	Skip	Email address of the IAM user that can be used as a login credential. IAM users can bind an email address after they are created. This parameter is mandatory if you select Set by user for Credential Type .
Mobile Number	Skip	(Optional) Mobile phone number of the IAM user that can be used as a login credential. IAM users can bind a mobile number after they are created.

2. Specify the access type.

Figure 2-2 Specifying the access type



Table 2-2 Access types

Access Type	Example	Description
Programmatic access	Select it.	This type allows access to cloud services using development tools, such as APIs, CLI, and SDKs, and requires an access key or password.
Management console access	Select it.	This type allows access to cloud services by using the management console and requires a password. If you select this parameter, Password must be selected for Credential Type .

3. Configure the credential type.

Figure 2-3 Credential types

Credential Type	 	Access key You can download the access key after you create the user.
	~	Password
		○ Set now
		Automatically generated
		A password will be automatically generated. You can download the password file and provide it to the user.
		Set by user
		A one-time login URL will be emailed to the user. The user can then click on the link to set a password.
		USB Key Give your account a security boost.

Table 2-3 Credential types

Cred Type	ential	Example	Description
Acces	ss key	Select it.	An access key comprises an AK and SK, and is used as a long-term identity credential to sign your requests for Huawei Cloud APIs .
			After users are created, you can download the access keys (AK/SK) generated for these users.
Pas swo rd	Set now	-	You need to set a password for the user and determine whether to require the user to reset the password at first login.
			If you will use the IAM user by yourself, you are advised to select this option, set a password, and deselect Require password reset at first login .
	Automati cally generate d	-	The system automatically generates a login password for the user. After the user is created, download the EXCEL password file and provide the password for the user. The user can then use this password for login.
			The password file must be downloaded upon the user creation. If you cancel the download, the password file cannot be obtained again. You can change the password of an IAM user by referring to Changing the Password of an IAM User.
			This option is available only when you create a single user.

Credential Type		Example	Description
Set by Select it. user		Select it.	A one-time login URL will be emailed to the user. The user can click the link to log in to the console and set a password.
			If you do not use the IAM user, select this option and enter the email address and mobile number of the IAM user. The user can then set a password by clicking the one-time login URL sent over email. The login URL is valid for seven days.
USB Key		Deselect it.	A USB key is a device that stores user credentials. You can use a USB key, rather than a password to verify your identity. This option is more secure, as there is no password to be leaked.
			Once selected, the USB key is the only way for the IAM user to log in. The password will be invalidated and can no longer be used.

- 4. Enable or disable login protection. This function is available only when **Access Type** is **Management console access**. In this example, select **Enable**.
 - Login protection enabled: IAM users need to enter verification codes in addition to their usernames and passwords during console login. For the best possible security, this two-factor identity authentication is recommended.

You can choose from SMS-, email-, and virtual MFA-based login verification.

Figure 2-4 Enable

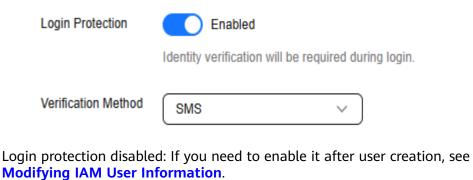


Figure 2-5 Login protection disabled

Login Protection



Identity verification will not be required during login.

- 5. Enable or disable API login protection. This function is available when only login protection is enabled and the verification mode is set to virtual MFA.
 - API login protection enabled: Both a password and a virtual MFA device are required to obtain an IAM user token. To obtain an IAM user token using both a password and a virtual MFA device, see Obtaining a User Token Through Password and Virtual MFA Authentication.
 - API login protection disabled: You can enable API login protection after user creation. Locate the target user, and click Security Settings in the

Operation column. In the displayed tab, click \checkmark next to **Verification Method** of the **Login Protection** function, enable this function, and select **Virtual MFA device**.

Step 3 Click **Next** and add the user to the developer user group.

s / Create User	nal) Add User to Group 3 Finish		
Users will automatically inherit permiss	sions from all the user groups to which you add them. You car	also create new groups.	
Available User Groups (3)	Enter a group name. Q	Selected User Groups (1)	Enter a group name. Q
User Group Name/Description		User Group Name/Description	Operation
admin Full permissions		Developer 	×
test-group			
Developer			
			Previous Cancel Crea

Figure 2-6 Adding the user to the user group

- **Step 4** Click **Create**. The created IAM user is displayed in the user list.
- **Step 5** In the displayed **Download Password** dialog box, click **OK** to download the initial password of the IAM user. Then, provide the account name, IAM username, and the IAM user's initial password for corresponding employees.

Figure 2-7 Downloading the password

Use	rs / Create User	(V) (Optional) Adv	User to Group — Users created su download and via password or you	oad Password cccessfully. This is the only time y eve the password. If you do not do download the password and mis new password later. Cancel Back to User Liat	ownload the		
	Users (Total: 1)						
>	Username	Email Address	Mobile Number	AK		Operation Result	
	Alice		-			Oreated	

Step 2: Log In to the Console as an IAM User

After an IAM user is created, employees can log in to Huawei Cloud as the IAM user. If an IAM user fails to log in, they can contact the administrator to **reset their password**.

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

HUAWEI ID login	IAM User Login
Phone/Email/Login ID/HUAWEI CLOUD account name	Company-A
Password 🕲	Alice
LOG IN	······
Register Forgot password?	Log In
Use Another Account	Forgot Password Remember me
our account and network information will be used to help improve our login experience. Learn more	Use Another Account: HUAWEI ID Federated User

Figure 2-8 Logging in as an IAM user

Table 2-4 Login parameters

Parameter	Example	Description
Tenant name or Huawei Cloud account name	Company-A	Account used to create the IAM user, for example, Company-A.
IAM username or email address	Alice	IAM username or email address entered during the user creation. You can obtain the IAM username and IAM user's initial password from the administrator.
IAM user password	****	Password of the IAM user, rather than the account. Enter the downloaded password.

Step 2 Click **Log In** to log in to Huawei Cloud as IAM user **Alice**.

- **Step 3** Verify the permissions of IAM user **Alice**.
 - 1. Switch to **CN-Hong Kong**.
 - 2. Choose **Elastic Cloud Server** from the service list to go to the ECS console. If the IAM user can perform all operations such as creating and managing ECSs, the ECS FullAccess permissions have been configured successfully.

- 3. Choose **Object Storage Service** from the service list. If the IAM user can view the bucket list and query bucket locations on the OBS console but cannot create OBS buckets, the OBS OperateAccess permissions have been configured successfully.
- 4. If the IAM user chooses any service other than ECS and OBS, and the system displays a message indicating insufficient permissions, the permissions have been configured successfully.
- 5. Switch to a region other than **CN-Hong Kong**. If the IAM user can only access the OBS homepage (cannot access ECS and other services), the permissions have been successfully assigned to the region-specific project.

----End