Identity and Access Management

Getting Started

Issue	09
Date	2024-12-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Notice

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

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

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:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Creating a User Group and Assigning Permissions

Scenario

If you do not want to create an account for every personnel 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 multiple IAM users for different enterprise personnel and assign permissions based on their job responsibilities. For the definitions of an account and IAM user, see **Basic Concepts**.

The following shows how to use IAM to manage permissions.

Process Flow

Procedure	Description
Preparations	Sign up for Huawei Cloud 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, skip this step. 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.

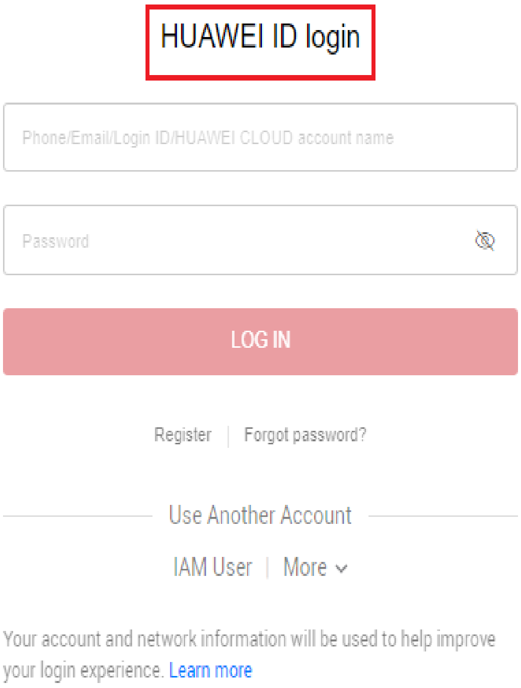
3. NOTE

IAM is a free service. There is no charge to use IAM.

Step 1: Create a User Group

Step 1 Use your HUAWEI ID to enable Huawei Cloud services, and then log in to Huawei Cloud.

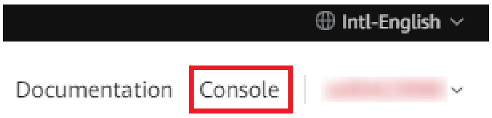
Figure 1-1 Logging in to Huawei Cloud



Your account and network information will be used to help improve your login experience. Learn more

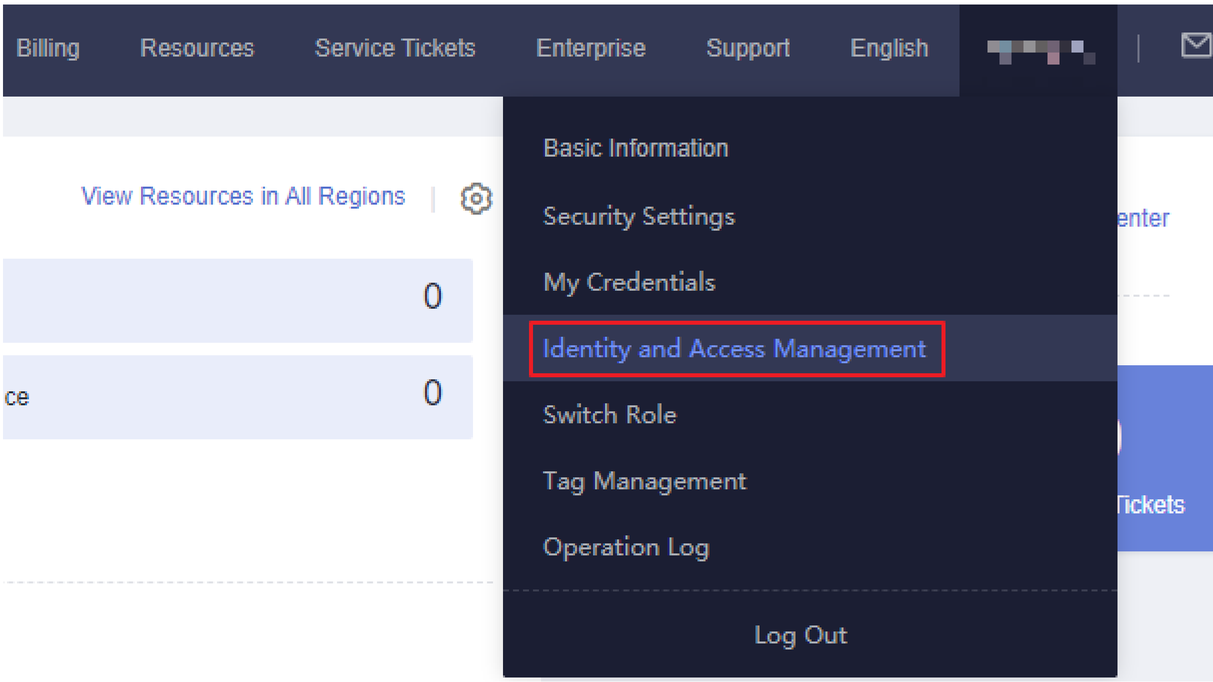
Step 2 Log in to the management console.

Figure 1-2 Logging in to the management console



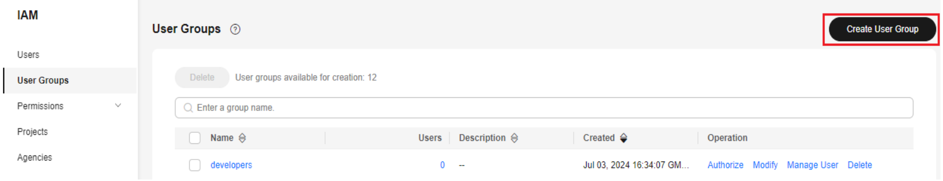
Step 3 On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.

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



User Groups

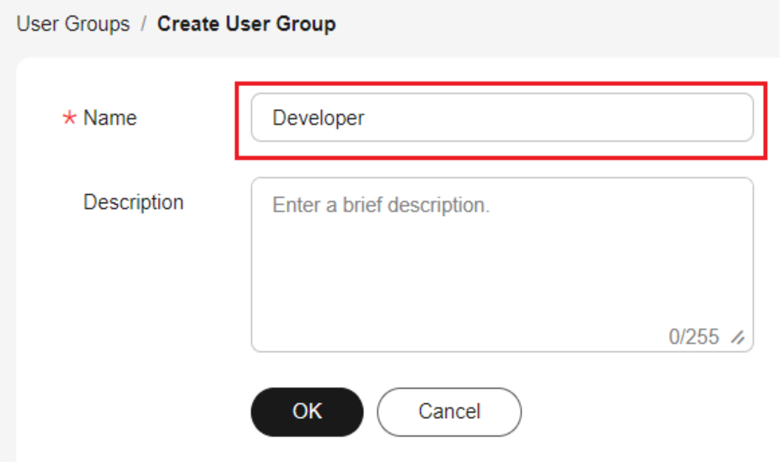
User groups available for creation: 12

Enter a group name.

□	Name	Users	Description	Created	Operation
□	developers	0	--	Jul 03, 2024 16:34:07 GM...	Authorize Modify Manage User Delete

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

Figure 1-5 Setting the user group details



* Name: Developer

Description: Enter a brief description.

0/255

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

You will be redirected to the user group list and the created 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, RDS, ELB, VPC, EVS, and OBS, so the administrator needs to perform the following operations to assign the required permissions to the developer 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.

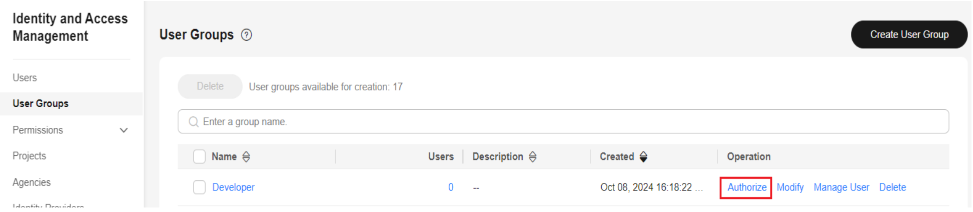
Table 1-1 lists the required permissions. You can determine which permissions are required by referring to **System-defined Permissions**. Regions are geographic areas where services are deployed. If a project-level service policy is attached to a user group for a project in a specific region, the policy takes effect only for that project.

Table 1-1 Required permissions

Cloud Service	Region	Policy or Role
ECS	Specific regions	ECS FullAccess
RDS	Specific regions	RDS FullAccess
ELB	Specific regions	ELB FullAccess
VPC	Specific regions	VPC FullAccess
EVS	Specific regions	EVS FullAccess
OBS	Global	OBS OperateAccess

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

Figure 1-6 Authorizing a user group



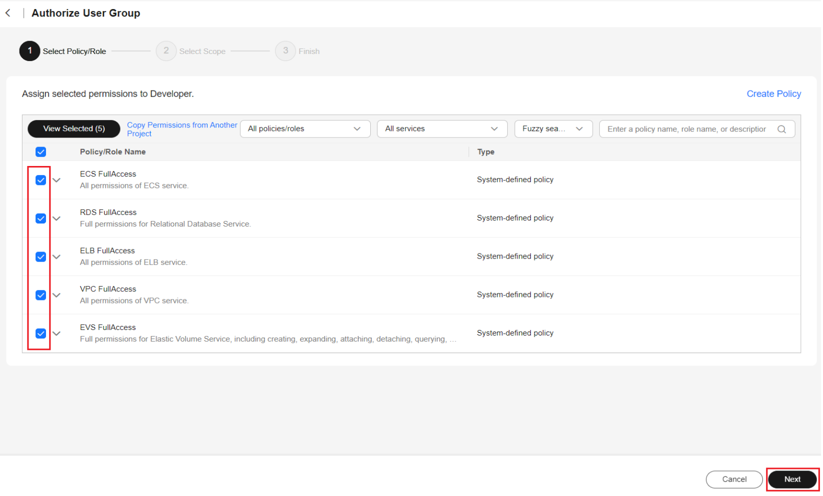
User groups available for creation: 17

Name	Users	Description	Created	Operation
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. All the services in **Table 1-1** except OBS are deployed in specific projects. Select desired permissions for project-level services and click **Next**.

Figure 1-7 Selecting required permissions



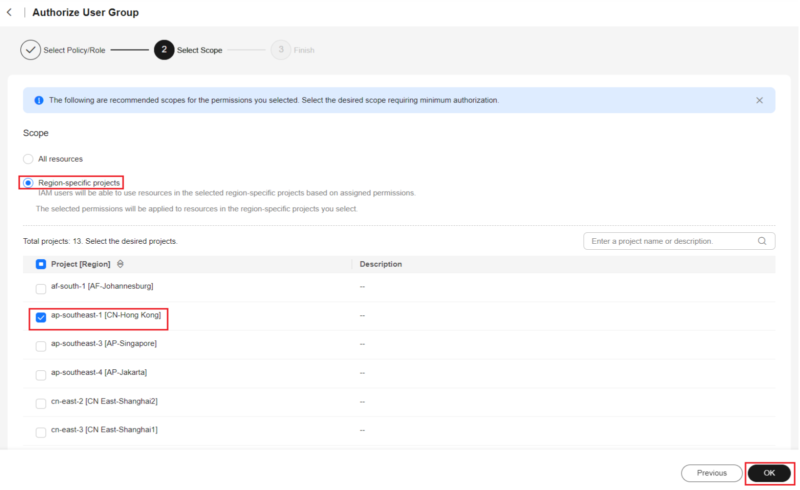
Assign selected permissions to Developer.

☑	Policy/Role Name	Type
☑	ECS FullAccess All permissions of ECS service.	System-defined policy
☑	RDS FullAccess Full permissions for Relational Database Service.	System-defined policy
☑	ELB FullAccess All permissions of ELB service.	System-defined policy
☑	VPC FullAccess All permissions of VPC service.	System-defined policy
☑	EVS FullAccess Full permissions for Elastic Volume Service, including creating, expanding, attaching, detaching, querying, ...	System-defined policy

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

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

Figure 1-8 Specifying the permission scope



The following are recommended scopes for the permissions you selected. Select 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 based on assigned permissions.

The selected permissions will be applied to resources in the region-specific projects you select.

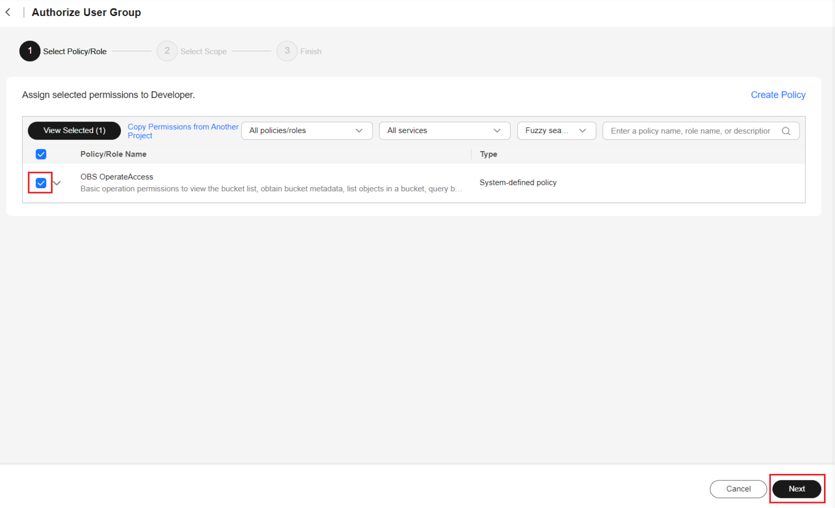
Total projects: 13. Select the desired projects.

Project [Region]	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]	--

Step 4 Assign permissions to the user group for the global services.

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

Figure 1-9 Selecting OBS OperateAccess



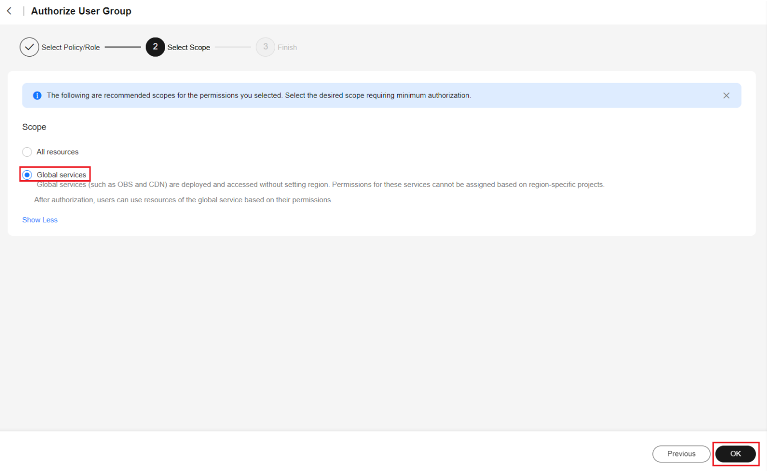
Assign selected permissions to Developer.

Create Policy
View Selected (1)
Copy Permissions from Another Project
All policies/roles
All services
Fuzzy sea...
Enter a policy name, role name, or descriptior

☑	Policy/Role Name	Type
☑	OBS OperateAccess Basic operation permissions to view the bucket list, obtain bucket metadata, list objects in a bucket, query b...	System-defined policy

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

Figure 1-10 Specifying the permission scope



The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

○ All resources

● Global services

Global services (such as OBS and CDN) are deployed and accessed without setting region. Permissions for these services cannot be assigned based on region-specific projects.

After authorization, users can use resources of the global service based on their permissions.

----End

2 Creating an IAM User and Logging In

Scenario

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

Process Flow

Procedure	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.

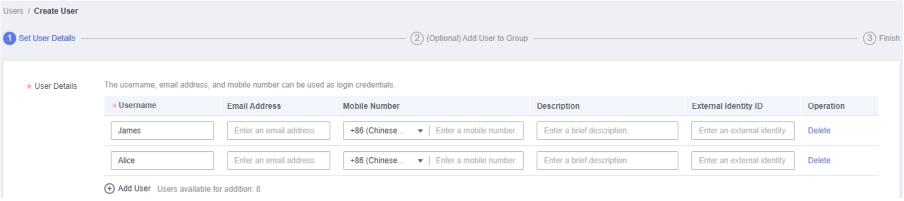
Step 1: Create an IAM User

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

Step 2 Specify the user details and access type.

1. Enter a user name.

Figure 2-1 Configuring user information



* User Details

The username, email address, and mobile number can be used as login credentials.

* Username	Email Address	Mobile Number	Description	External Identity ID	Operation
James	Enter an email address.	+86 (Chinese... Enter a mobile number.	Enter a brief description.	Enter an external identity	Delete
Alice	Enter an email address.	+86 (Chinese... Enter a mobile number.	Enter a brief description.	Enter an external identity	Delete

⊕ Add User Users available for addition: 8

NOTE

IAM users can log in to Huawei Cloud using the username, email address, or mobile number.

Table 2-1 User details

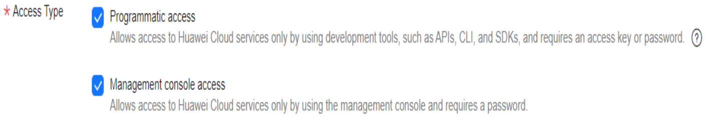
Parameter	Example	Description
Username	Alice	(Mandatory) Username used by an IAM user to log in to Huawei Cloud.
Email Address	Skip	Email address of the IAM user that can be used as a login credential. IAM users can bind an email address after they are created. This parameter is mandatory if you select **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.
External Identity ID	Skip	Identity of an enterprise user in IAM user SSO. This parameter is mandatory if virtual user SSO via SAML is configured for an IAM user. It can contain a maximum of 128 characters.

2. Specify 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**.

Figure 2-2 Specifying the access type



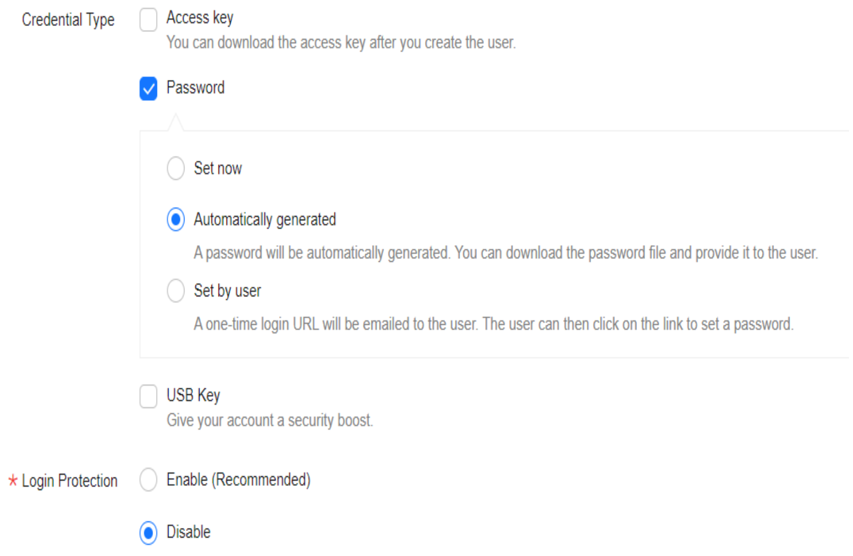
* Access Type

☑ Programmatic access
Allows access to Huawei Cloud services only by using development tools, such as APIs, CLI, and SDKs, and requires an access key or password. ?

☑ Management console access
Allows access to Huawei Cloud services only by using the management console and requires a password.

3. Specify the credential type and login protection.

Figure 2-3 Specifying the credential type and login protection



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.

* Login Protection ○ Enable (Recommended)

● Disable

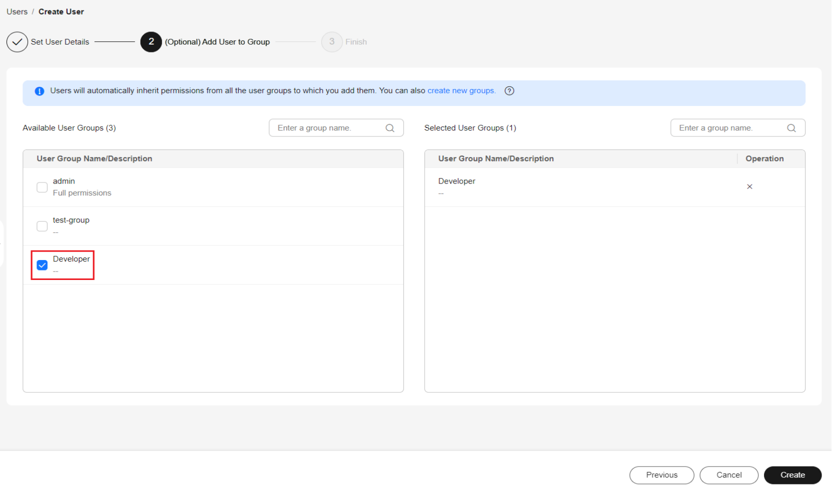
Table 2-3 Specifying the credential type and login protection

Credential Type and Login Protection		Example	Description
Access key		Deselect it.	After you create the user, you can download the **access key (AK/SK)** generated for the user. Each user can have a maximum of two access keys.
Password	Set now	A password set by the account	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**.
	Automatically generated	An automatically generated password	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. This option is available only when you create a single user.

Credential Type and Login Protection		Example	Description
	Set by user	A password set by the IAM user	A one-time login URL will be emailed to the user. The user can click on 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 on the one-time login URL sent over email. The login URL is valid for seven days.
Login Protection	Enable (Recommended)	-	If login protection is enabled, the user will need to enter a verification code in addition to the username and password during login. Enable this function for account security. You can choose from SMS-, email-, and virtual MFA–based login verification.
	Disable	-	To enable login protection for an IAM user after creation, see **Viewing or Modifying IAM User Information**.

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

Figure 2-4 Adding the user to the user group



Users / **Create User**

✓ Set User Details — 2 (Optional) Add User to Group — 3 Finish

Users will automatically inherit permissions from all the user groups to which you add them. You can also create new groups.

Available User Groups (3) | Enter a group name.

	User Group Name/Description
□	admin Full permissions
□	test-group --
☑	Developer --

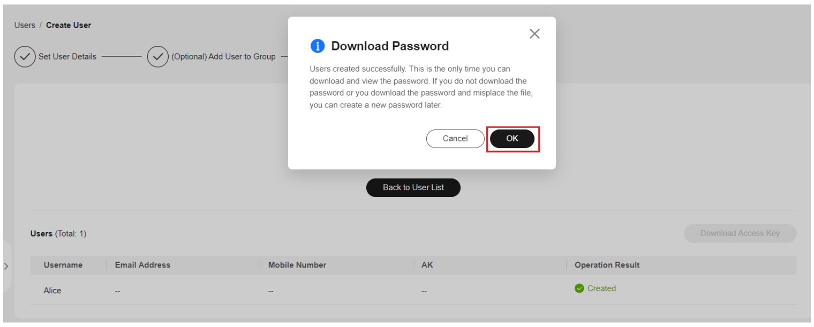
Selected User Groups (1) | Enter a group name.

User Group Name/Description	Operation
Developer --	×

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 2-5 Downloading the password



Download Password

Users created successfully. This is the only time you can download and view the password. If you do not download the password or you download the password and misplace the file, you can create a new password later.

Users (Total: 1)

Username	Email Address	Mobile Number	AK	Operation Result
Alice	--	--	--	✓ Created

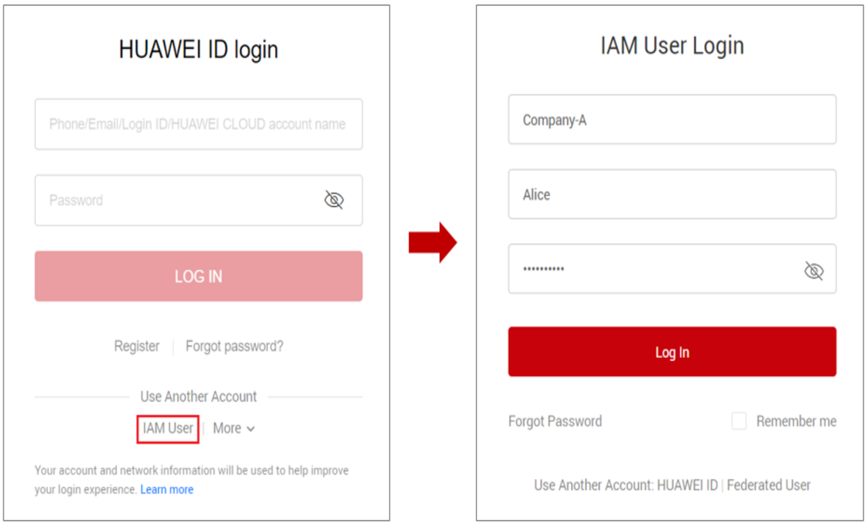
----End

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 user name or email address**, and **IAM user password**.

Figure 2-6 Logging in as an IAM user



Your account and network information will be used to help improve your login experience. Learn more

Company-A

Alice

••••••••••

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.

Parameter	Example	Description
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**.

----End