

Identity and Access Management

Getting Started

Issue 08
Date 2021-03-27



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



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 Before You Start.....	1
2 Step 1: Create User Groups and Assign Permissions.....	3
3 Step 2: Create IAM Users and Log In.....	7
4 Change History.....	12

1 Before You Start

Reading this document will help you to:

- Create Identity and Access Management (IAM) users.
- Create user groups based on your organization's business functions.
- Assign permissions to user groups.
- Create IAM users for employees in your organization.
- Enable IAM users to log in to Huawei Cloud.

Prerequisites

You already have an account. If you do not have an account, create one.

Example Scenario

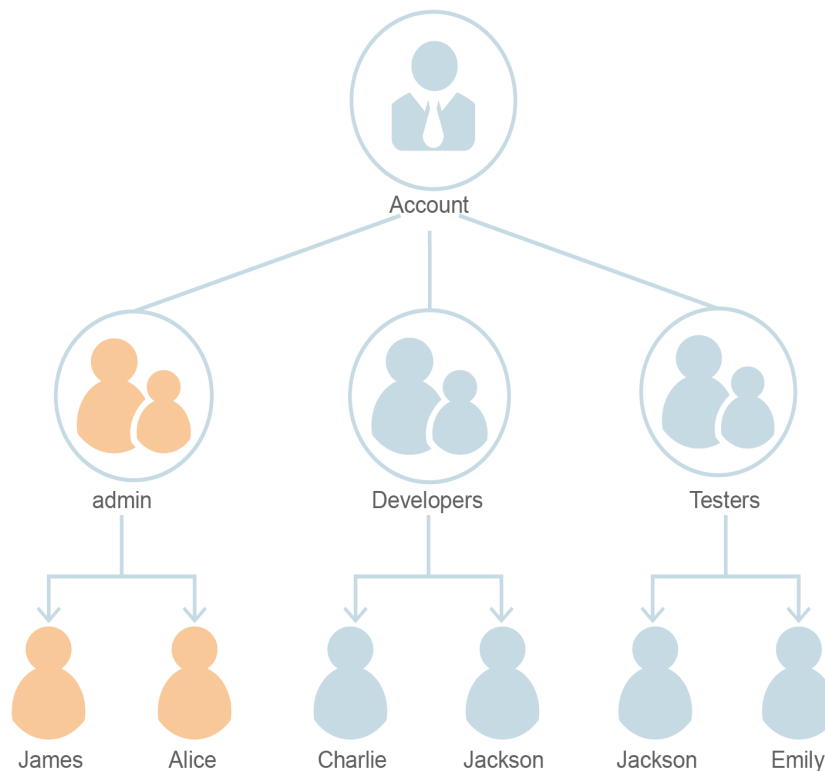
A website development company has three functional teams in Hong Kong. With IAM, the company's administrator can create only one account and then use this account to create IAM users for employees and assign permissions based on their job responsibilities. For the definitions of an account and IAM user, see [Basic Concepts](#).

The following uses the company as an example to show how to use IAM to manage permissions.

Organizational Structure

- Management team (**admin** group in [Figure 1-1](#)): manages employees and resources, assigns permissions, and allocates resources. The team members include James and Alice.
- Development team (**Developers** group in [Figure 1-1](#)): develops websites. The team members include Charlie and Jackson.
- Test team (**Testers** group in [Figure 1-1](#)): tests websites. The team members include Jackson and Emily. Jackson develops and tests websites, so he needs to join both the **Developers** and **Testers** groups to obtain the required permissions.

Figure 1-1 User management model



User Groups and Required Resources

- **admin** group: manages user permissions using IAM.
- **Developers** group: develops websites using Elastic Cloud Server (ECS), Elastic Load Balance (ELB), Virtual Private Cloud (VPC), Relational Database Service (RDS), Elastic Volume Service (EVS), and Object Storage Service (OBS).
- **Testers** group: performs functional and performance testing on websites by using the Application Performance Management (APM) service.

User Management Process

1. The company's administrator logs in to Huawei Cloud, creates user groups **Developers** and **Testers**, and grants them permissions. For details, see [Step 1: Create User Groups and Assign Permissions](#).
2. The administrator creates IAM users for members of the three functional teams. The members then log in to Huawei Cloud as IAM users. For details, see [Step 2: Create IAM Users and Log In](#).

2 Step 1: Create User Groups and Assign Permissions

A company has three functional teams, including the management (**admin** group), development, and test teams. After the company administrator creates an account, the default group **admin** is automatically generated and has full permissions for all cloud services. The administrator only needs to create another two groups in IAM for the development and test teams, respectively.

Creating User Groups

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

Figure 2-1 Logging in to Huawei Cloud

HUAWEI ID login

Phone/Email/Login ID/HUAWEI CLOUD account name

Password

LOG IN

Register | Forgot password

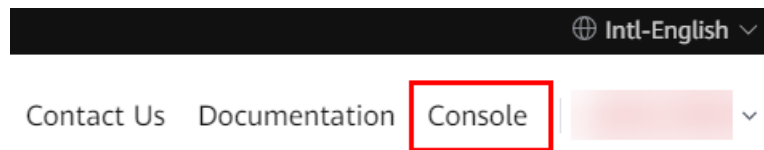
Use Another Account

IAM User | Federated User | Huawei Website Account |
Huawei Enterprise Partner | HUAWEI CLOUD Account

Your account and network information will be used to help improve your login experience. [Learn more](#)

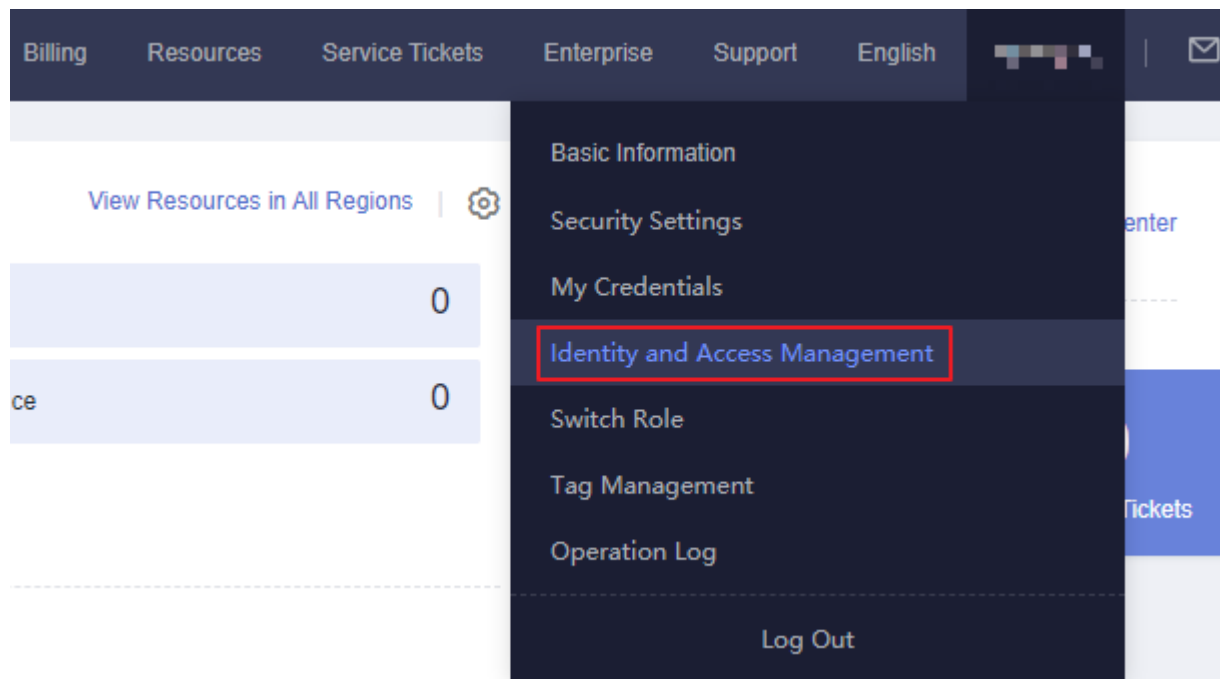
Step 2 Log in to the management console.

Figure 2-2 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 2-3 Accessing the IAM console



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

Figure 2-4 Creating a user group



Step 5 Create a group for developers and click **OK**.

Figure 2-5 Setting the user group details

Step 6 Repeat steps [Step 4](#) and [Step 5](#) to create a group for testers.

----End

Assigning Permissions to User Groups

Developers in the company need to use ECS, RDS, ELB, VPC, EVS, and OBS, so the administrator needs to assign the required permissions to the developer group to enable access to these services. Testers in this company need to use APM, so the administrator needs to assign the required permissions to the tester group to enable access to the service. After permissions are assigned, users in the two groups can access the corresponding services. For details about the permissions of all cloud services, see [System-defined Permissions](#).

Step 1 Determine the permissions policies to be attached to each user group.

Determine the policies (see [Table 2-1](#)) 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.

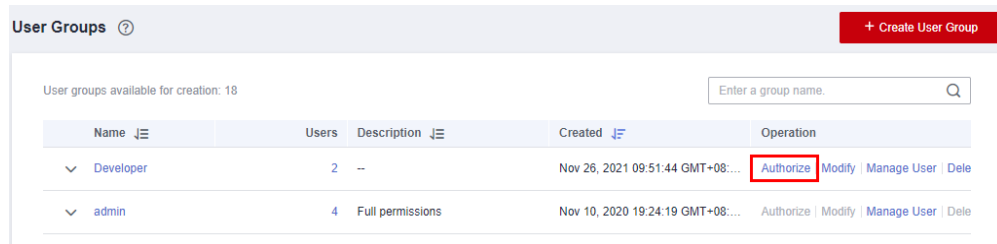
Table 2-1 Required permissions policies

User Group	Cloud Service	Region	Policy or Role
Developer group	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

User Group	Cloud Service	Region	Policy or Role
Tester group	APM	Specific regions	APM FullAccess

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

Figure 2-6 Authorizing a user group



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

1. All the services in **Table 2-1** except OBS are deployed in specific projects. Select desired permissions for project-level services and click **Next**.
2. Select **Region-specific projects** for **Scope**, select **CN-Hong Kong**, and click **OK**.

The company is located in Hong Kong. Therefore, select **CN-Hong Kong** to reduce network latency and accelerate service access. Then users in the developer group can access the specified project-level services in **CN-Hong Kong** but do not have permissions to access the services in other regions.

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

1. Select OBS OperateAccess and click **Next**.
2. Select **Global services** for **Scope** and click **OK**.

Step 5 Repeat steps **Step 2** to **Step 4** to attach the **APM FullAccess** policy to the tester group in the **CN-Hong Kong** region.

----End

3 Step 2: Create IAM Users and Log In

Create IAM users for employees and add the users to the user groups created in the previous section. Each IAM user has their own password to log in to Huawei Cloud, and can use resources based on the assigned permissions.

Creating IAM Users

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

Step 2 Specify the user details and access type. To create more users, click **Add User**. A maximum of 10 users can be created at a time.

Figure 3-1 Configuring user information

The screenshot shows the 'Create User' interface with a table for user details. The table has the following columns: Username, Email Address, Mobile Number, Description, External Identity ID, and Operation. Two rows are shown for users named James and Alice. The 'Mobile Number' column has a dropdown menu with '+86 (Chinese...)' selected. Below the table, there is an 'Add User' button and a note 'Users available for addition: 8'.

NOTE

- Users can log in to Huawei Cloud using the username, email address, or mobile number.
- If users forget their password, they can reset it through email address or mobile number verification. If no email addresses or mobile numbers have been bound to users, users need to request the administrator to reset their passwords.

Table 3-1 User information

Parameter	Description
Username	Username that will be used to log in to Huawei Cloud, for example, James and Alice . This field is required.
Email Address	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 field is required if you have selected Set by user for Credential Type .

Parameter	Description
Mobile Number	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. This field is optional.
Description	Additional information about the IAM user. This field is optional.
External Identity ID	Identity of an enterprise user in IAM user SSO. The value contains a maximum of 128 characters. This field is mandatory when you configure IAM user SSO for federated login.

Figure 3-2 Setting 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. [Learn more](#)

Management console access
Allows access to HUAWEI CLOUD services only by using the management console and requires a password.

Access key
You can download the access key after you create the user.

Password

Set now

 Require password reset at first login
 Automatically generated
A password will be automatically generated and then sent to the user by email.
 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.

Login Protection
 Enable (Recommended)
Complete identity verification by to log in to the system.

Disable

- **Programmatic access:** Select this option to allow the user to access cloud services using development tools, such as APIs, CLI, and SDKs. You can generate an **access key** or set a **password** for the user.
- **Management console access:** Select this option to allow the user to access cloud services using the management console. You can set or generate a password for the user or request the user to set a password at first login.

 NOTE

- If the user **accesses cloud services only by using the management console**, select **Management console access** for **Access Type** and **Password** for **Credential Type**.
- If the user **accesses cloud services only through programmatic access**, select **Programmatic access** for **Access Type** and **Access key** for **Credential Type**
- If the user **needs to use a password as the credential for programmatic access** to certain APIs, select **Programmatic access** for **Access Type** and **Password** for **Credential Type**
- If the user needs to **perform access key verification** when using certain services in the console, such as creating a data migration job in the Cloud Data Migration (CDM) console, select **Programmatic access** and **Management console access** for **Access Type** and **Access key** and **Password** for **Credential Type**.

Table 3-2 Setting the credential type and login protection

Credential Type and Login Protection		Description
Access key		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	Set a password for the user and determine whether to require the user to reset the password at first login. If you are the user, select this option and set a password for login. You do not need to select Require password reset at first login .
	Automatically generated	The system automatically generates a login password for the user. After the user is created, download the EXCEL password file and provide the password to the user. The user can then use this password for login. This option is available only when you create a single user.
	Set by 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 .

Credential Type and Login Protection		Description
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 (Optional) Click **Next** to add the users to specific user groups.

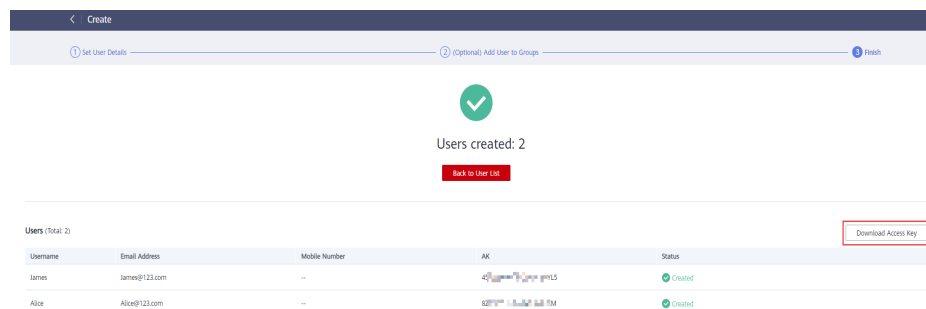
- The users will inherit the permissions assigned to the user groups.
- You can also create new groups as required.

 **NOTE**

The default user group **admin** has the administrator permissions and the permissions required to use all cloud resources. For mapping between the company employees and user groups, see [Figure 1-1](#).

Step 4 Click **Create**. If you have selected **Programmatic access** for **Access Type** and have selected **Access key** for **Credential Type** (see [Table 3-2](#)), you can download the access keys in the **Finish** step.

Figure 3-3 Users created successfully



Step 5 Repeat steps [Step 1](#) through [Step 4](#) to create users Charlie, Jackson, and Emily, and add them to the corresponding groups.

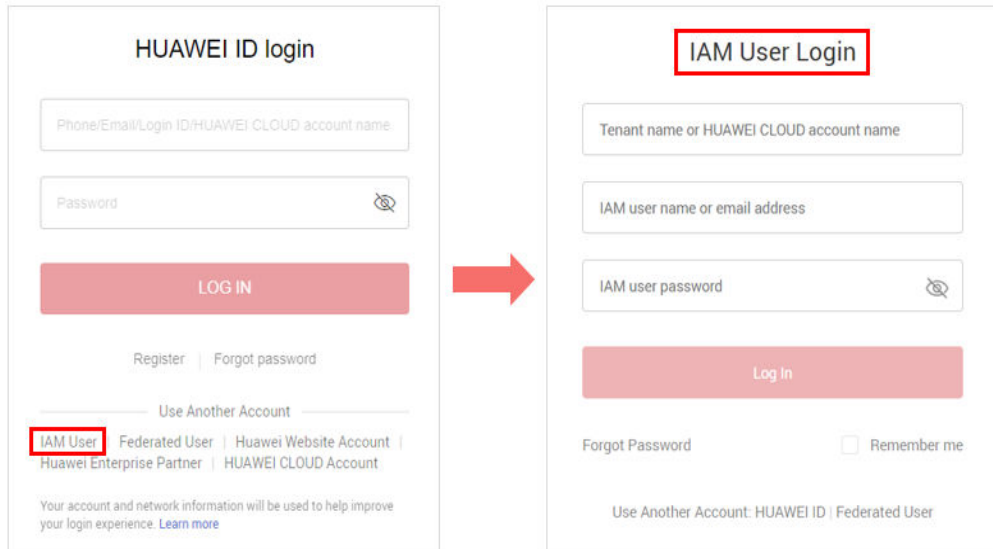
----End

IAM User Login

After creating users (for example, **James**, **Alice**, **Charlie**, **Jackson**, and **Emily**), the administrator needs to provide the account name, IAM user names, and IAM users' initial passwords to corresponding employees. Employees can use their own usernames and passwords to access Huawei Cloud. If an IAM user login fails, 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 3-4 Logging in as an IAM user



- **Tenant name or HUAWEI CLOUD account name:** the name of the account that was used to create the IAM user.
- **IAM user name or email address:** the username (for example, **James**) or email address of the IAM user. You can obtain the username and password from the administrator.
- **IAM user password:** the password of the IAM user (not the password of the account)

Step 2 Click **Log In**.

----End

4 Change History

Table 4-1 Change history

Released On	Description
2021-11-30	This issue is the tenth official release, which incorporates the following change: Modified section Step 1: Create User Groups and Assign Permissions according to optimization of the authorization function.
2021-09-02	This issue is the ninth official release, which incorporates the following change: Optimized section Step 1: Create User Groups and Assign Permissions according to changes to the permissions management function.
2021-03-27	This issue is the eighth official release, which incorporates the following change: Updated the document based on the new feature of HUAWEI ID login.
2020-12-30	This issue is the seventh official release, which incorporates the following change: Updated the document based on changes in the login page, security settings function, and UI strings.
2020-10-27	This issue is the sixth official release, which incorporates the following change: Updated the screenshots of the login page based on the login method change.

Released On	Description
2020-06-08	This issue is the fifth official release, which incorporates the following change: Updated the following sections to include descriptions about HUAWEI ID login: Step 1: Create User Groups and Assign Permissions Step 2: Create IAM Users and Log In
2020-02-10	This issue is the fourth official release, which incorporates the following change: Modified section Step 1: Create User Groups and Assign Permissions based on policy name changes.
2020-01-19	This issue is the third official release, which incorporates the following change: Modified section Step 1: Create User Groups and Assign Permissions based on console changes.
2019-06-06	This issue is the second official release, which incorporates the following change: Optimized the steps for assigning permissions in Step 1: Create User Groups and Assign Permissions .
2019-02-26	This issue is the first official release.