

# IAM Identity Center Best Practices

**Issue** 01  
**Date** 2025-07-08



**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**



HUAWEI 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.

## **Huawei Cloud Computing Technologies Co., Ltd.**

Address: Huawei Cloud Data Center Jiaoxinggong Road  
Qianzhong Avenue  
Gui'an New District  
Gui Zhou 550029  
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

---

# Contents

---

**1 Multi-Account Identity and Permissions Management Using IAM Identity Center**  
..... **1**

# 1 Multi-Account Identity and Permissions Management Using IAM Identity Center


## Overview

In this section, management account **A** is used to create a user **Alice** in the IAM Identity Center and associate it with member account **a\_\_abc** in the organization. The member account has been associated with the permission set **PolicySet** (configured with the ECS management permission). This case describes how to manage identity and permissions of multiple accounts.

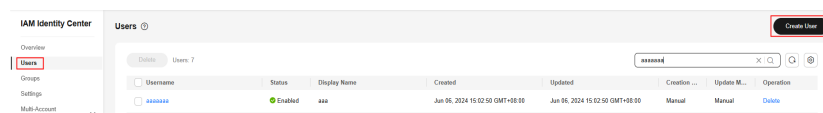
## Prerequisites

IAM Identity Center needs to obtain member account information from the organization created by the Organizations service. Before using IAM Identity Center, you must [enable the Organizations service and create an organization](#). Then, log in to IAM Identity Center using the organization's management account.

## Creating a User

- Step 1** Log in to the [Huawei Cloud console](#) using the organization's management account.
- 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 a user



- Step 5** Configure user information and 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.

Figure 1-2 Configuring user information

< | Create User

1 Set User Details 2 (Optional) Add User to Groups 3 Confirm

**User Details**

\* Username

\* Family Name

\* Given Name

\* Display Name  This is typically the full name of the workforce user.

\* Email Address  This email address will be used to receive password setup or reset instructions.

\* Confirm Email Address

\* Password ☐ Send an email to this user with password setup instructions. ☐ Generate a one-time password that you can share with this user.

✓ Contact Methods - Optional

✓ Job-related information - Optional

✓ Address - Optional

Table 1-1 Basic information

Parameter	Description
Username	IAM Identity Center username, for example, <b>Alice</b> . The value is user-defined and must be unique.
Password	Select a password generation method. <ul style="list-style-type: none"><li>● <b>Send an email to this user with password setup instructions:</b> The system will send an email to the user. The user can set a password following the instructions in the email.</li><li>● <b>Generate a one-time password that you can share with this user:</b> 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.</li></ul> <b>CAUTION</b> 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 <b>reset the password</b> .
Email Address	Email address of the 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 <b>Email Address</b> and <b>Confirm Email Address</b> must be the same.
Family Name	Family name of the user.

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

**Step 6** In the **Confirm** step, confirm the configuration and click **OK** in the lower right corner of the page. The created IAM Identity Center user is 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 1-3** Confirming user creation

< | Create User

✓ Set User Details

✓ (Optional) Add User to Groups

3 Confirm

User Details

UsernameAliceFamily Name

Given NameAliceDisplay NameAlice

Email Address

▼ Contact Methods - Optional


▼ Job-related Information - Optional

▼ Address - Optional

----End

## Creating a User Group

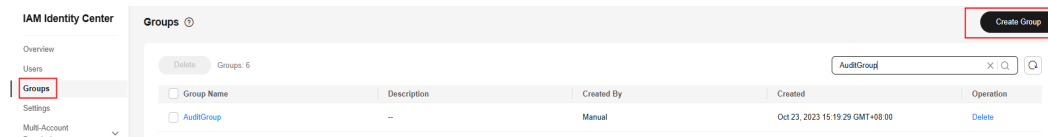
**Step 1** Log in to the [Huawei Cloud console](#) using the organization's management account.

**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 1-4** Creating a group



**Step 5** On the **Create Group** page, set **Group Name** (for example, **ere123**) and **Description**.

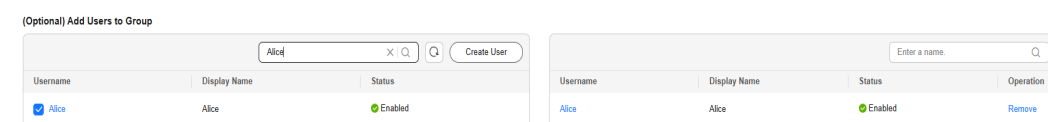
The group name must be unique in IAM Identity Center.

**Figure 1-5** Creating a group



**Step 6** (Optional) Select users to be added to this group.

**Figure 1-6** Adding a user



**Step 7** Click **OK**. The user group **ere123** is created and displayed in the user group list.

-----End

## Creating a Permission Set

**Step 1** In the navigation pane, choose **Multi-Account Permissions > Permission Sets**.

**Step 2** Click **Create Permission Set** in the upper right corner of the page.

**Figure 1-7** Creating a permission set



**Step 3** In the **Specify Details** step, configure the basic information for the permission set and click **Next**.

**Figure 1-8** Specifying permission set details

< Create Permission Set

A permission set contains policies that determine a user's permissions to access a Huawei Cloud account. When you associate a user or group with a permission set for a Huawei Cloud account, IAM Identity Center creates an IAM agency in the account and attaches the policies specified in the permission set to that agency. [Learn More](#)

1 Specify Details 2 Set Policy 3 Confirm

Name

Session Duration ☒ 1h ☐ 4h ☐ 8h ☐ 12h ☐ Custom

Custom duration

Initial Access Page

Description

011,624

**Table 1-2** Permission set details

Parameter	Description
Name	Name of a permission set, for example, <b>PolicySet</b> . The value is user-defined and must be unique.
Session Duration	The length of time a user can be logged in to the console. When the user's login duration exceeds the configured session duration, the user is automatically logged out. To maintain access, the user needs to log back in again.
Initial Access Page	The page a user lands on after login using the user portal URL. For example, if you enter the IAM console URL, users will land on the IAM console after login.
Description	Description of a permission set.

**Step 4** 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**, only identity policies are displayed in the system-defined policy list, and custom policy configuration box will not be displayed. If no identity policies are available for a cloud service, you can disable **Identity Policy Only**. Then, you can select identity policies and policies for some functions of the cloud service.

- **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 1-9** Setting policies

< | Create Permission Set

1 A permission set contains policies that determine a user's permissions to access a Huawei Cloud account. When you associate a user or group with a permission set for a Huawei Cloud account, IAM Identity Center creates an IAM agency in the account and attaches the policies specified in the permission set to that agency. [Learn More](#)

Specify Details — 2 Set Policy — 3 Confirm

Identity Policy Only ☒   
 You are advised to enable Identity Policy Only for more fine-grained, flexible permission control based on service requirements. If this function is disabled, you can configure a policy.

System-defined policies Not set   
 IAM provides system-defined policies that define the common actions of cloud services. You can directly choose from these IAM system-defined policies, but cannot modify them.

View Selected (0)

Policy Name	Type	Description
<input checked="" type="checkbox"/> ECSFullPolicy	Identity policy	All permissions of ECS service.

Custom identity policies Not set   
 Custom identity policies can be created to supplement system-defined identity policies for fine-grained permissions control.

Cancel Previous **Next**

**Step 5** In the **Confirm** step, confirm the configuration and click **OK** in the lower right corner.

**Figure 1-10** Confirming configuration

< | Create Permission Set

1 A permission set contains policies that determine a user's permissions to access a Huawei Cloud account. When you associate a user or group with a permission set for a Huawei Cloud account, IAM Identity Center creates an IAM agency in the account and attaches the policies specified in the permission set to that agency. [Learn More](#)

Specify Details — Set Policy — 3 Confirm

Specify Details

Name PolicySet

Session Duration 1h

Initial Access Page —

Description —

System-defined policies

Policy Name	Type	Description
<input checked="" type="checkbox"/> ECSFullPolicy	Identity policy	All permissions of ECS service.

Cancel Previous **OK**

### 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

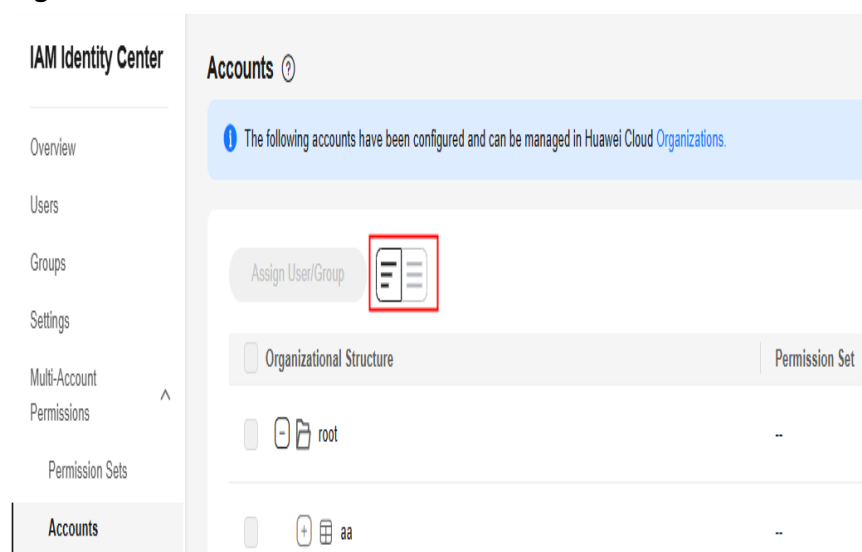
## Associating the Account with the User and Permission Set

**Step 1** In the navigation pane, choose **Multi-Account Permissions** > **Accounts**.

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

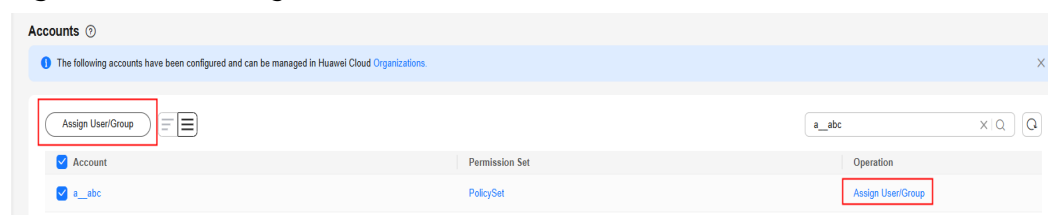


to switch to the list view.

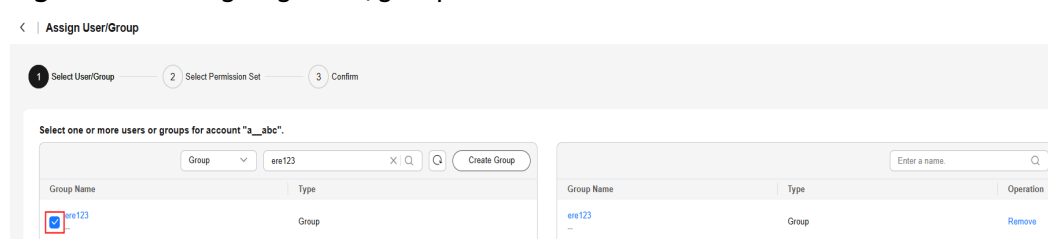
**Figure 1-11** Account view

**Step 2** In the account list, select account **a\_abc** and click **Assign User/Group** in the upper left corner.

Alternatively, locate a target account and click **Assign User/Group** in the **Operation** column.

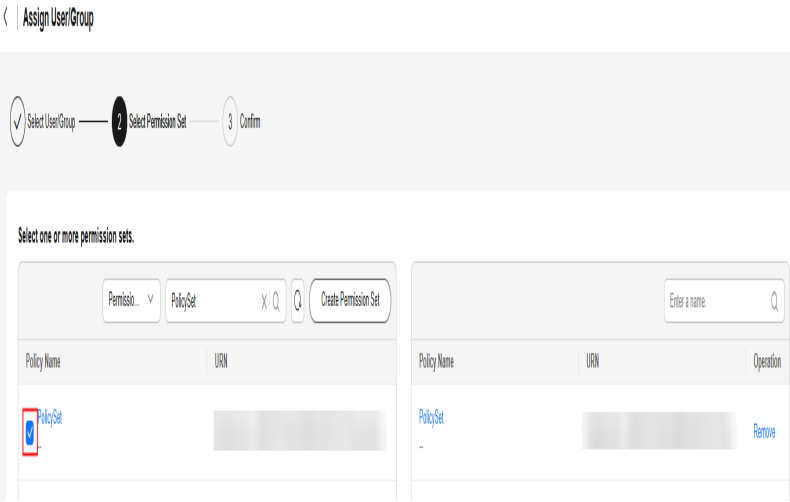
**Figure 1-12** Selecting an account

**Step 3** In the **Select User/Group** step, select one or more users/groups, for example, group **ere123**, and click **Next**.

**Figure 1-13** Assigning users/groups

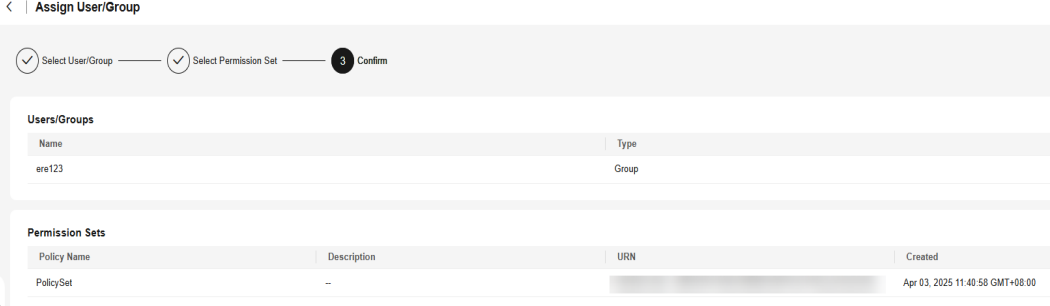
**Step 4** In the **Select Permission Set** step, select one or more permission sets and click **Next**.

Figure 1-14 Selecting one or more permission sets



**Step 5** In the **Confirm** step, confirm the configuration and click **OK**.

Figure 1-15 Confirming configuration

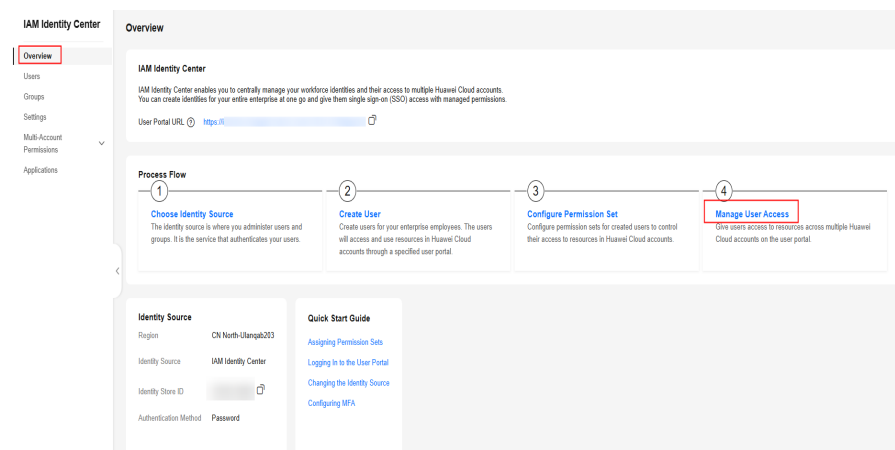


----End

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

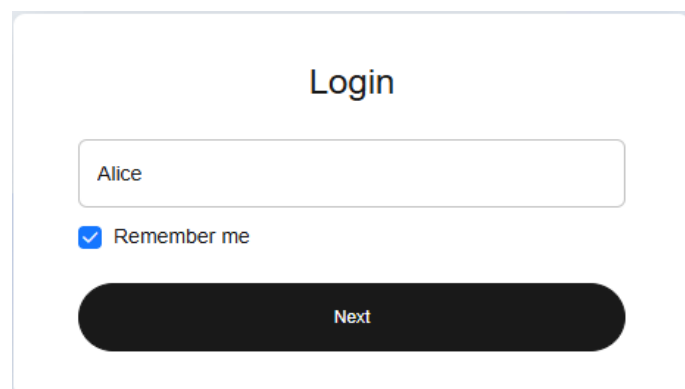
**Step 1** In the navigation pane, choose **Overview**, obtain the user portal URL, and send the URL to user **Alice**.

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

**Figure 1-16** Obtaining the user portal URL

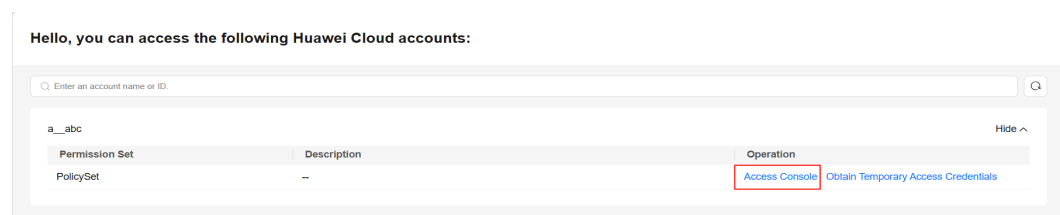
**Step 2** Open a browser and access the user portal URL. In this example, the user is **Alice**. Enter **Alice** for the IAM Identity Center username, and click **Next**.

The login password is obtained when **creating users**. If the password is forgotten or needs to be changed, the administrator can **reset the password** for another password setup instruction email or a new one-time password.

**Figure 1-17** User login

**Step 3** Enter the password, and click **Log In**.

**Step 4** Click **Access Console** in the **Operation** column to access the ECS resources controlled by the permission set **PolicySet** of the account.

**Figure 1-18** Accessing resources

----End