Organizations

# User Guide

| | |
|---|---|
| **Issue** | 01 |
| **Date** | 2025-07-17 |

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

## Trademarks and Permissions

## 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 Permissions Management

## 1.1 Creating an IAM User and Granting Organizations Permissions

This section describes how a management account creates an IAM user and grants organization administrator permissions to the user.

You can use **Identity and Access Management (IAM)** for fine-grained permissions control on Organizations. With IAM, you can:

- Grant users only the permissions required to perform a given task based on their job responsibilities. For example, you use the management account to create two IAM users, and assign one of them the permissions to create and delete OUs while the other one only the permission to view information about OUs.
- Use the management account to create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials to access Huawei Cloud and use Organizations, improving account security.
- Entrust another Huawei Cloud account or a cloud service to perform efficient O&M on your Organizations.

If your HUAWEI ID or Huawei Cloud cloud account meets your permissions requirements, you can skip this section.

The following describes how to create an IAM user and grant permissions to the user. **Figure 1-1** illustrates an example process.

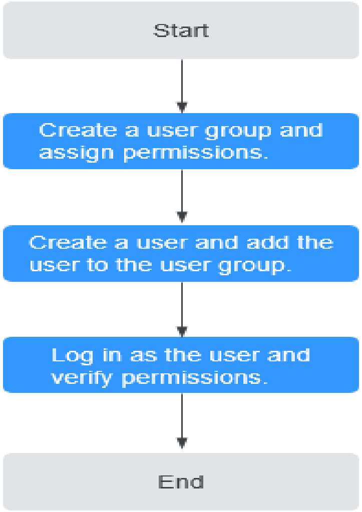
### Prerequisites

Before assigning permissions to user groups, learn about the permissions supported by Organizations, as described in **Permissions**.

For the permissions of other services, see **System Permissions**.

### Process Flow

**Figure 1-1** Process of granting Organizations permissions


Start
Create a user group and assign permissions.
Create a user and add the user to the user group.
Log in as the user and verify permissions.
End

1. On the IAM console, **Create a user group and assign permissions**.

   Create a user group on the IAM console to assign the **Organizations ReadOnlyAccess** permission to the group.

2. **Create an IAM user and add it to the user group**.

   Create a user on the IAM console and add it to the user group created in **1**.

3. **Log in** and verify permissions.

   Log in to the console as the IAM user. If you can access Organizations and view organization information but encounter an error message when you attempt to add an OU, saying "Insufficient permission. Contact the administrator", the **Organizations ReadOnlyAccess** policy has been applied and you have only the permission to view organization information.

# 1.2 Creating Custom Policies

You can create custom policies to supplement the system-defined policies of Organizations. For the actions that can be added to custom policies, see **Policies and Supported Actions**.

To create a custom policy, choose either visual editor or JSON.

- Visual editor: Select cloud services, actions, resources, and request conditions. There is no need to know much about policy syntax.
- JSON: Edit policies from scratch or based on an existing policy in JSON format.

For details, see **Creating a Custom Policy**. The following lists examples of common Organizations custom policies.

## Example Custom Policies

- Example 1: Grant permission to invite member accounts to join an organization or to remove member accounts from an organization.

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:accounts:invite",
                "organizations:accounts:remove"
            ]
        }
    ]
}
```

- Example 2: Grant permission to deny the deletion of OUs or removal of member accounts.

  To apply a policy with only Deny statements, it must be used together with other policies. If you do not assign the permission to perform an action, the action is denied by default. If the permissions granted to an IAM user contain both Allow and Deny, **the Deny statements take precedence over the Allow statements**.

  Assume that you want to grant the permissions of the **OrganizationsFullAccess** policy to a user but want to prevent them from deleting OUs or removing member accounts. You can create a custom policy for denying the deletion, and attach this policy together with the **OrganizationsFullAccess** policy to the user. As an explicit Deny in any policy overrides any kind of Allow, the user can perform all operations on a given organization except deleting its OUs or removing member accounts. The following is an example of a deny policy:

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:ous:delete",
                "organizations:accounts:remove"
            ]
        }
    ]
}
```

# 2 Managing Organizations

## 2.1 Overview of Organizations

### What Is Organizations?

An organization is an entity that you create to manage multiple accounts. Each organization is composed of exactly one management account, multiple member accounts, and one root with many OUs organized in a hierarchical, tree-like structure. You can group member accounts into the root or any of the OUs. For details about the basic concepts of Organizations, see **Basic Concepts**.

Helpful links:

- **Creating an Organization**: You can use your current account as the management account to create an organization and invite other accounts to join your organization.
- **Viewing Details About an Organization**: You can view details about your organization, root, OUs, and accounts.
- **Deleting an Organization**: You can delete an organization when you no longer need it.

## 2.2 Creating an Organization

You can use a Huawei Cloud account as the management account to create an organization. After creating the organization, you can **invite existing accounts** or **create new accounts** to add them to your organization, and you can **create OUs** to manage accounts in your organization.

### Prerequisites

The current account has not joined any organization. If this account is already in an organization and you still need to use it, remove it from the current organization and then use it to create your organization. For how to remove from an organization, see **Leaving an Organization As a Member Account**.

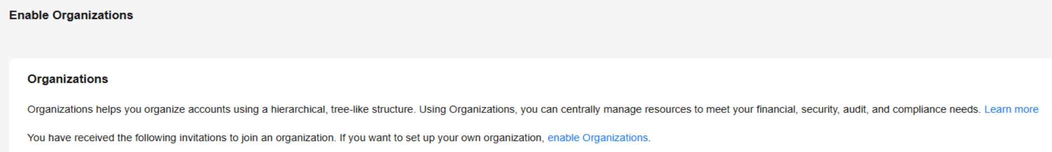
The current account must have enabled Enterprise Center and become an enterprise master account. For details, see **Enabling Enterprise Center**.

## Procedure

You can create an organization on the management console or by **calling Organizations APIs**. The following describes how to create an organization on the console.

**Step 1** Log in to Huawei Cloud, and navigate to the Organizations console.

**Step 2** Go to the page for enabling the Organizations service, and click **enable Organizations**.



Enable Organizations

Organizations

Organizations helps you organize accounts using a hierarchical, tree-like structure. Using Organizations, you can centrally manage resources to meet your financial, security, audit, and compliance needs. Learn more

You have received the following invitations to join an organization. If you want to set up your own organization, enable Organizations.

After the Organizations service is enabled, your organization and the root are automatically created, and your login account is defined as the management account.

**----End**

Then, you can **invite existing accounts to join your organization** or **create new accounts in your organization**, and you can also **create OUs** to manage accounts.

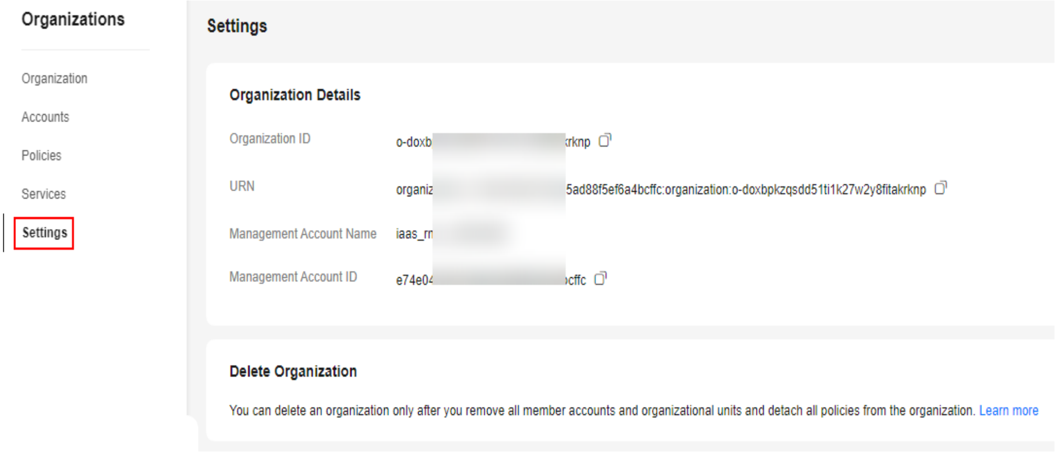
# 2.3 Viewing Details About an Organization

You can use the management account to view all information about your organization. The member accounts can view only the organization ID, management account name, and management account ID.

## Viewing Organization Details from the Management Account

Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Settings** page to view information such as the organization ID, URN, management account name, and management account ID.

**Figure 2-1** Viewing organization details from the management account



Settings

Organization Details

Organization ID o-doxb[redacted]krknp

URN organiz[redacted]5ad88f5ef6a4bcffc:organization:o-doxbpkzqsdd51ti1k27w2y8fitakrknp

Management Account Name iaas_m[redacted]

Management Account ID e74e04[redacted]bcffc

Delete Organization

You can delete an organization only after you remove all member accounts and organizational units and detach all policies from the organization. Learn more

## Viewing Root Details from the Management Account

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Click the organization root. You can view details about the root on the right of the organization tree, including the root ID, time of creation, URN, policies, and tags.

**----End**

## Viewing OU Details from the Management Account

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Click the OU. You can view details about the OU on the right of the organization tree, including the OU name, ID, URN, when the OU was created, as well as policies and tags attached.

**----End**

## Viewing Account Details from the Management Account

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Click the account. You can view details about the selected account on the right of the organization tree, including the account name, account ID, URN, time when the account joined the organization, parent OU, as well as policies, tags, and agency services associated with the account.

**----End**

### Viewing Organization Details from a Member Account

Log in to Huawei Cloud as a member account, navigate to the Organizations console, and access the **Settings** page to view the organization ID, URN, management account name, and management account ID.

## 2.4 Deleting an Organization

### Prerequisites

You can delete an organization when you no longer need it.

**NOTE**

An organization can be deleted only after all member accounts, OUs, and policies are removed from the organization.

### Impacts

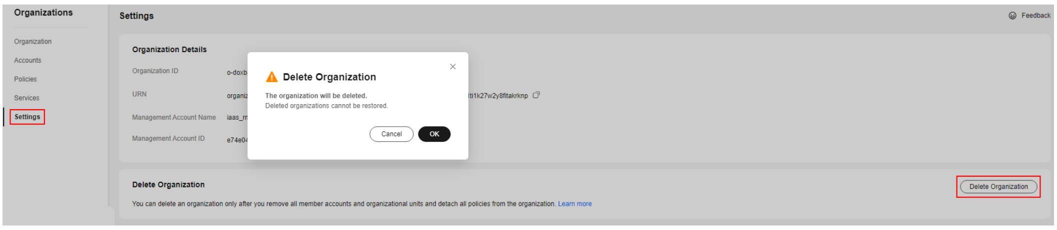
- **Impacts on the Management Account**
  - The management account will become a standalone account. You can use it to create a different organization or accept an invitation from another organization to add the account to that organization as a member account.
  - The management account of an organization is never affected by service control policies (SCPs). There is no change to the permissions assigned to the management account and its IAM users.
- **Impact on Member Accounts**
  - Each member account will become a standalone account. You can use it to create a different organization or accept an invitation from another organization to add the account to that organization as a member account.
  - After the organization is deleted, member accounts are no longer affected by SCPs, and the permissions assigned to the member accounts and their IAM users may change.
- **Impact on Policies**
  - If you delete an organization, you cannot recover it. If you have created SCPs inside the organization, they are also deleted and you cannot recover them.

### Procedure

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Settings** page.

**Step 2** Click **Delete Organization**. In the displayed dialog box, click **OK**.

**Figure 2-2** Deleting an organization



Organization Details

Organization ID o-doxb

URN organiz ti1k27w2y8fitakrknp

Management Account Name iaas_m

Management Account ID e74e04

Delete Organization

The organization will be deleted.
Deleted organizations cannot be restored.

Delete Organization

You can delete an organization only after you remove all member accounts and organizational units and detach all policies from the organization. Learn more

**----End**

# 3 Managing OUs

## 3.1 Overview of an OU

### What Is an OU?

An organizational unit (OU) is a container or a logical grouping of accounts in your organization. You can use OUs to group accounts together to administer them as a single unit. An OU can be mapped to a department, a subsidiary, or a project team. You can create OUs within other OUs. Each OU can have only one parent OU, but they can have many other child OUs or member accounts.

Helpful links:

- **Creating an OU**
- **Modifying an OU**
- **Viewing Details About an OU**
- **Deleting an OU**

## 3.2 Creating an OU

You can create an OU in your organization's root. OUs can be nested up to five levels deep.

To create an OU:

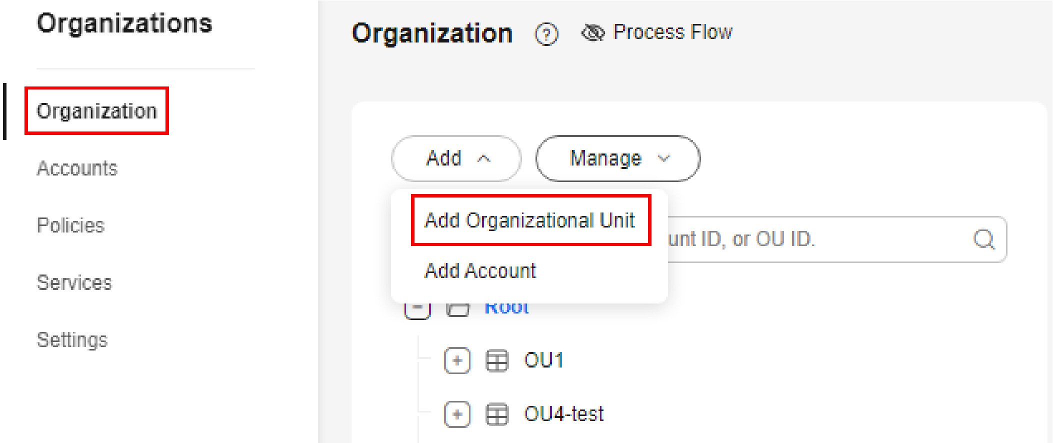
**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the parent OU by clicking its name rather than the expand icon. If you are creating an OU for the first name, select the **Root** OU.

OUs can be nested up to five levels deep. Each OU can have only one parent OU but can have many child OUs. When creating an OU, ensure that the parent OU you select is the upper-level one.

**Step 3** Choose **Add** > **Add Organizational Unit**.

**Figure 3-1** Adding an OU



**Step 4** In the displayed dialog box, enter the OU name.

**Step 5** (Optional) Add a tag to the OU.

A tag consists of a key-value pair. Tags are used to identify, classify, and search for OUs. A maximum of 20 tags can be added to an OU.

**Table 3-1** describes the key and value descriptions of a tag.

**Table 3-1** Tag description

| Element | Description | Example |
|---|---|---|
| Tag key | A tag key of an OU must be unique. You can create a custom key or select a key of an existing tag created in Tag Management Service (TMS).<br>A tag key:<br>● Cannot be an empty string.<br>● Contains 1 to 128 characters.<br>● Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF). | Key_0001 |
| Tag value | A tag value can be repetitive or an empty string.<br>A tag value:<br>● Can be an empty string.<br>● Contains 1 to 225 characters.<br>● Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF). | Value_0001 |

**Step 6** Click **OK**.

**----End**

# 3.3 Modifying an OU

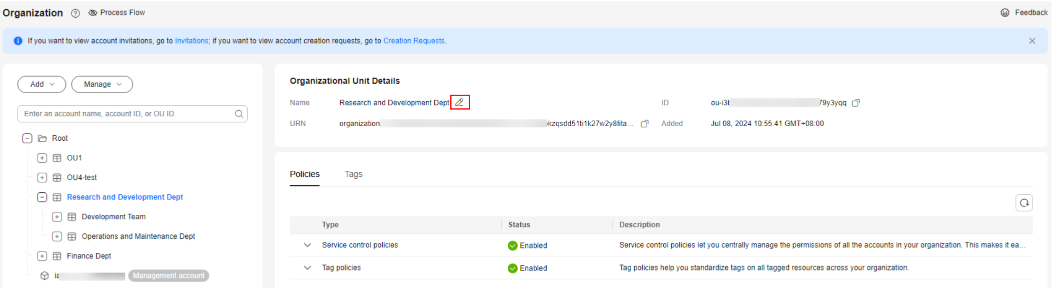
After an OU is created, you can modify its name, tag, and policy at any time. For details about how to modify tags and policies, see **Managing Tags** and **Attaching or Detaching an SCP**.

## Procedure

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the OU you want to rename and click 🖉 next to the OU name on the displayed OU details page.

**Figure 3-2** Renaming an OU



If you want to view account invitations, go to Invitations; if you want to view account creation requests, go to Creation Requests.

Enter an account name, account ID, or OU ID.

- Root
  - OU1
  - OU4-test
  - Research and Development Dept
    - Development Team
    - Operations and Maintenance Dept
  - Finance Dept
  - ia[redacted] Management account

Organizational Unit Details

Name Research and Development Dept 🖉
ID ou-i3t[redacted]79y3yqq
URN organization[redacted]kzqsdd51ti1k27w2y8fita...
Added Jul 08, 2024 10:55:41 GMT+08:00

| Type | Status | Description |
|---|---|---|
| Service control policies | Enabled | Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it ea... |
| Tag policies | Enabled | Tag policies help you standardize tags on all tagged resources across your organization. |

**Step 3** Enter a new name for the OU and click ✓ to save it.

**----End**

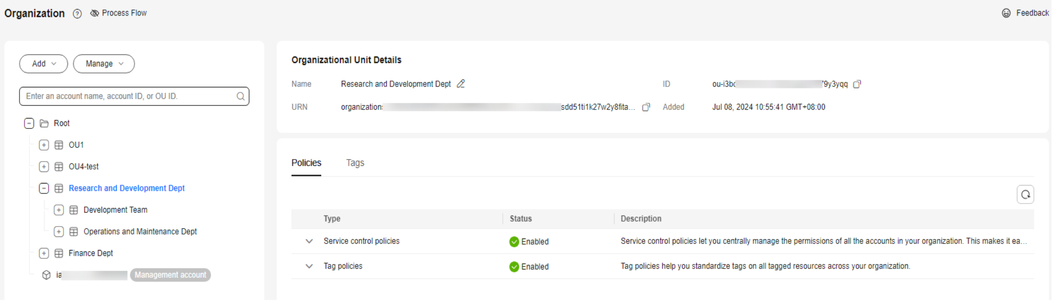
# 3.4 Viewing Details About an OU

After an OU is created, you can view its details any time by following the steps below.

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Click the OU you want to view. Its details are displayed on the right of the OU tree, including the OU name, ID, URN, time of creation, policies, and tags.

**Figure 3-3** Viewing details about an OU



Organizational Unit Details

Name Research and Development Dept

ID ou-i3bc[redacted]'9y3yqq

URN organization:[redacted]sdd51ti1k27w2y8fita...

Added Jul 08, 2024 10:55:41 GMT+08:00

| Type | Status | Description |
|---|---|---|
| Service control policies | Enabled | Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it ea... |
| Tag policies | Enabled | Tag policies help you standardize tags on all tagged resources across your organization. |

**----End**

# 3.5 Deleting an OU

You can delete an OU that is no longer needed.

NOTE

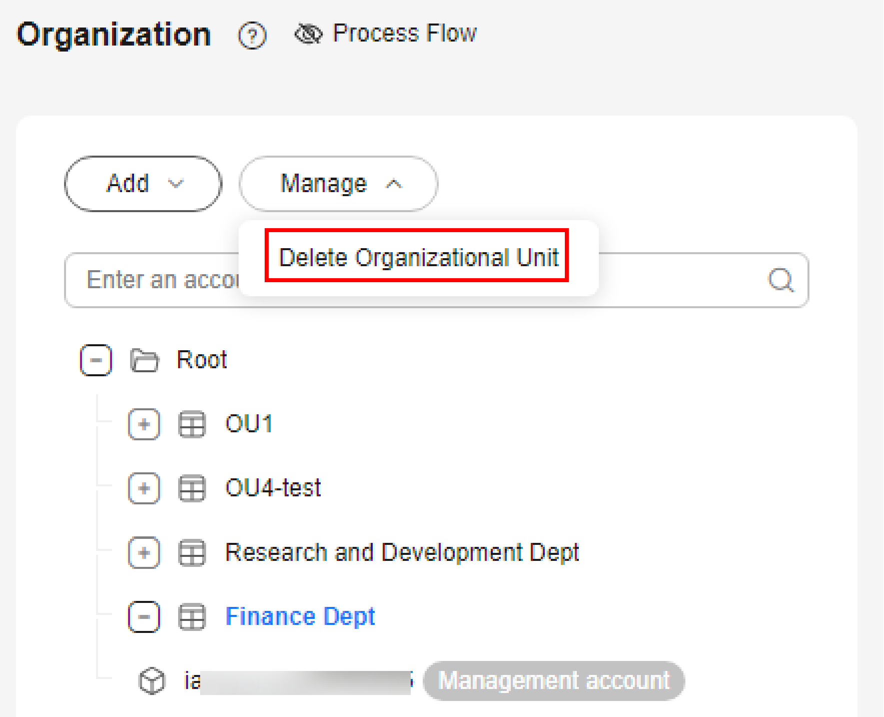
You cannot delete an OU if it contains other OUs or accounts.

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Click the OU you want to delete and click **Manage** above the OU tree.

**Step 3** Choose **Delete Organizational Unit**. In the displayed dialog box, click **OK**.

**Figure 3-4** Deleting an OU



**----End**

# 4 Managing Accounts

## 4.1 Overview of an Account

### Accounts in Your Organization

An account is used to contain your Huawei Cloud resources. It is the smallest unit of an organization. Each organization has one management account and multiple member accounts.

**Table 4-1** Account types

| Account Type | Function | Quota |
|---|---|---|
| Management account | With the Organizations service, you can use the management account to create an organization and manage OUs, accounts, and policies for the organization. | 1 (Each organization can have exactly one management account.) |
| Member account | Except for the management account, other accounts in an organization are member accounts. Each member account is part of only one organization at a time. Generally, member accounts hold resources for a specific application or project of an organization. | 9 |

### Impacts of Being in an Organization

When you **invite an existing account to your organization** or **create a new account in your organization**, Organizations will automatically make the following changes to the new member account:

- A service-linked agency is created in the member account. It is a cloud service agency with the system-defined permission **OrganizationsServiceLinkedAgencyPolicy** for all resources.

- The permissions of the new member account are affected by service control policies and tag policies. You may have service control policies and tag policies attached to the root or the OU that contains the new member account. If so, the policies will apply to the new member account and all IAM users in the member account.
- When you use the management account to enable a trusted service, the trusted service can create a service-linked agency for that trusted service in the member account.

Helpful links:

- **Inviting an Account to Join Your Organization**: You can create invitations, manage invitations you have sent, and accept or reject invitations.
- **Creating an Account**: You can use the management account to create new accounts.
- **Closing an Account**: You can use the management account to close any unwanted accounts that you have created. Invited accounts cannot be closed.
- **Moving an Account**: You can move accounts from one OU to another OU.
- **Viewing Account Details**: You can view the account name, account ID, the time when it joined an organization, any account-owing OUs, and the policies, tags, and delegated services that are attached to the account.
- **Removing a Member Account from Your Organization**: You can use the management account to remove member accounts from your organization.
- **Viewing Account Invitation/Creation Records**: When you sign in to the management account of your organization, on the **Accounts** page, you can view account details, including the account list, creation records, and invitations. You can also invite, create, close, move, and remove accounts and cancel any pending invitations.

# 4.2 Inviting an Account to Join Your Organization

When you invite a HUAWEI ID or Huawei Cloud account to join your organization, Organizations sends an invitation to the ID or account owner, who then chooses to accept or reject the invitation. You can use the Organizations console to issue and manage invitations that you send to other accounts.

NOTE

The accounts you invite to join your organization must have completed enterprise or individual real-name authentication. For details, see **Real-Name Authentication**.

The original accounting relationship (master-member association) of invited accounts will remain unchanged.

This section includes the following content:

- **Issuing Invitations to Accounts**
- **Managing Open Invitations of Your Organization**
- **Accepting or Rejecting an Invitation from an Organization**

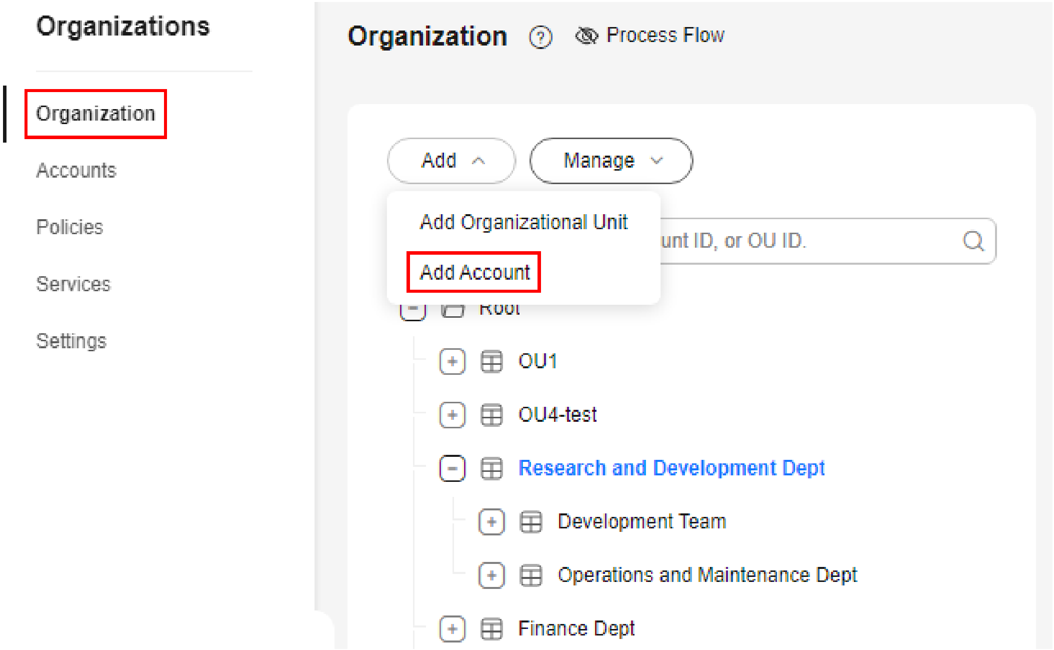
## Issuing Invitations to Accounts

To invite other accounts to join your organization, perform the steps described in this section. By default, those invited accounts will be placed as member accounts in the root OU. If you want to move them to another OU, see **Moving an Account**.

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** On the **Organization** page, choose **Add** > **Add Account**.

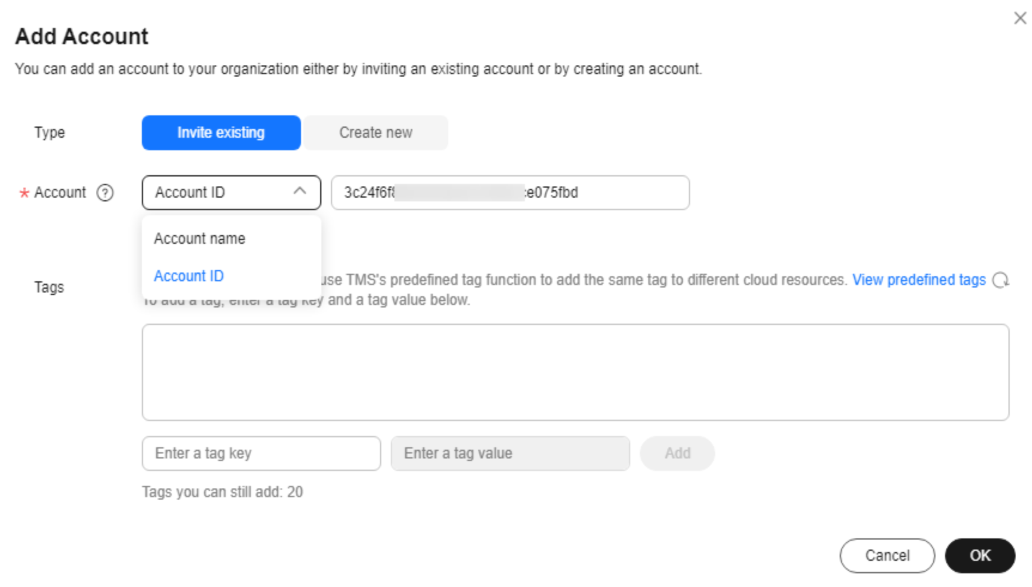
**Figure 4-1** Adding an account



**Step 3** In the displayed dialog box, select **Invite existing** and enter the name or ID of the account you want to invite.

For details about how to obtain an account name or ID, see **Obtaining Account ID and Name**.

**Figure 4-2** Inviting an existing account



Add Account

You can add an account to your organization either by inviting an existing account or by creating an account.

Type: Invite existing | Create new

* Account: Account ID — 3c24f6f[redacted]e075fbd

Tags: …use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

…and a tag value below.

Tags you can still add: 20

**Step 4** (Optional) Add one or more tags to the account.

A tag consists of a key-value pair. Tags are used to identify, classify, and search for accounts. You can add up to 20 tags to an account.

Table 4-2 describes the key and value descriptions of a tag.

**Table 4-2** Tag description

| Element | Description | Example |
|---|---|---|
| Tag key | A tag key of an account must be unique. You can create a custom key or select a key of an existing tag created in Tag Management Service (TMS).<br>A tag key:<br>● Cannot be an empty string.<br>● Contains 1 to 128 characters.<br>● Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF). | Key_0001 |
| Tag value | A tag value can be repetitive or an empty string.<br>A tag value:<br>● Can be an empty string.<br>● Contains 1 to 225 characters.<br>● Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF). | Value_0001 |

**Step 5** Click **OK** to send an invitation to the invited account.

**----End**

## Managing Open Invitations of Your Organization

When you log in as the management account, you can view and manage invitations of your organization.

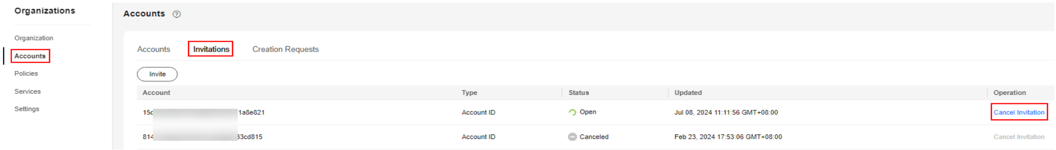
**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Accounts** page.

**Step 2** Click the **Invitations** tab. You can view all the invitations sent from your organization and their statuses on the page.

**Step 3** Locate the **Open** invitation you want to cancel and click **Cancel Invitation** in the **Operation** column. Then, click **OK** in the displayed dialog box.

After the invitation is canceled, its status changes from **Open** to **Canceled**. If you want that account to join your organization again, you must send a new invitation.

**Figure 4-3** Canceling an invitation



| Account | Type | Status | Updated | Operation |
|---|---|---|---|---|
| 15c[redacted]1a8e821 | Account ID | Open | Jul 08, 2024 11:11:56 GMT+08:00 | Cancel Invitation |
| 814[redacted]33cd815 | Account ID | Canceled | Feb 23, 2024 17:53:06 GMT+08:00 | Cancel Invitation |

**----End**

## Accepting or Rejecting an Invitation from an Organization

Your account may receive an invitation to join an organization. You can accept or reject the invitation.

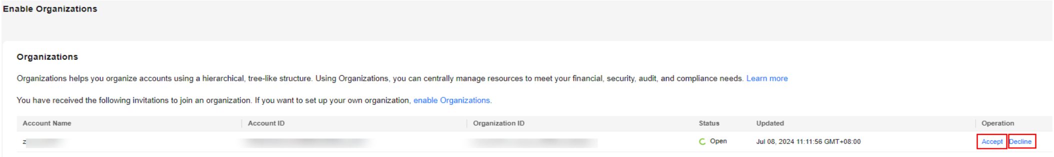
NOTE

Each account can join only one organization. If you receive multiple invitations, you can accept only one of them. If you have joined an organization, you need to exit that organization before accepting an invitation from another organization.

**Step 1** Log in to Huawei Cloud as an invited member account, and navigate to the Organizations console.

**Step 2** Locate the target invitation and click **Accept** or **Decline** in the **Operation** column. Then, click **OK** in the displayed dialog box.

**Figure 4-4** Accepting or rejecting an invitation



Enable Organizations

Organizations

Organizations helps you organize accounts using a hierarchical, tree-like structure. Using Organizations, you can centrally manage resources to meet your financial, security, audit, and compliance needs. Learn more

You have received the following invitations to join an organization. If you want to set up your own organization, enable Organizations.

| Account Name | Account ID | Organization ID | Status | Updated | Operation |
|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | Open | Jul 08, 2024 11:11:56 GMT+08:00 | Accept Decline |

**----End**

# 4.3 Creating an Account

You can use the management account to create new accounts in your organization. The accounts you created are referred to as resource accounts.

This section includes the following content:

- **Creating an Account**
- **Accessing Account Resources Via Agency**
- **Accessing Account Resources Via IAM Identity Center**

## Constraints

- An organization administrator can create a maximum of five accounts at a time.
- The email address associated with the account you are creating cannot be used by another account.
- Accounts created via Organizations can only be used for login only by switching roles via an agency or by accessing the IAM Identity Center console.
- The accounting of accounts created via Organizations is hosted by the organization management account by default.

⚠ CAUTION

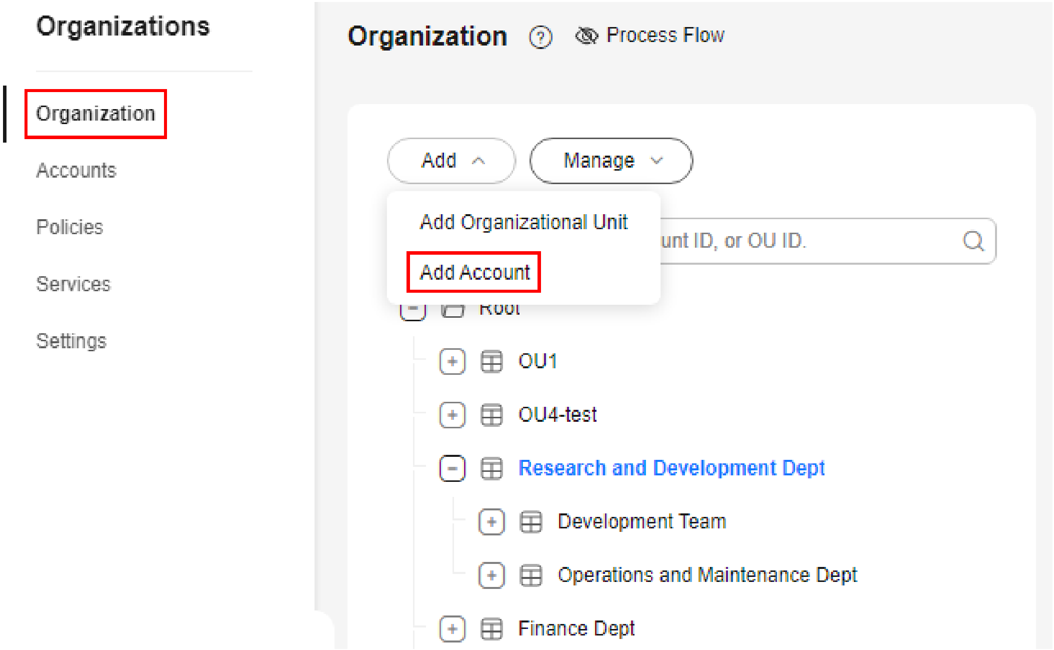
- The email address to be associated with the new account must be valid.
- An agency will be created in the new account created via Organizations for the management account. You can delete this agency in the new account. Before deleting the agency, enable IAM Identity Center and configure related identities and permissions to ensure that the service owner can access the account.

## Creating an Account

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** On the **Organization** page, choose **Add** > **Add Account**.

**Figure 4-5** Adding an account

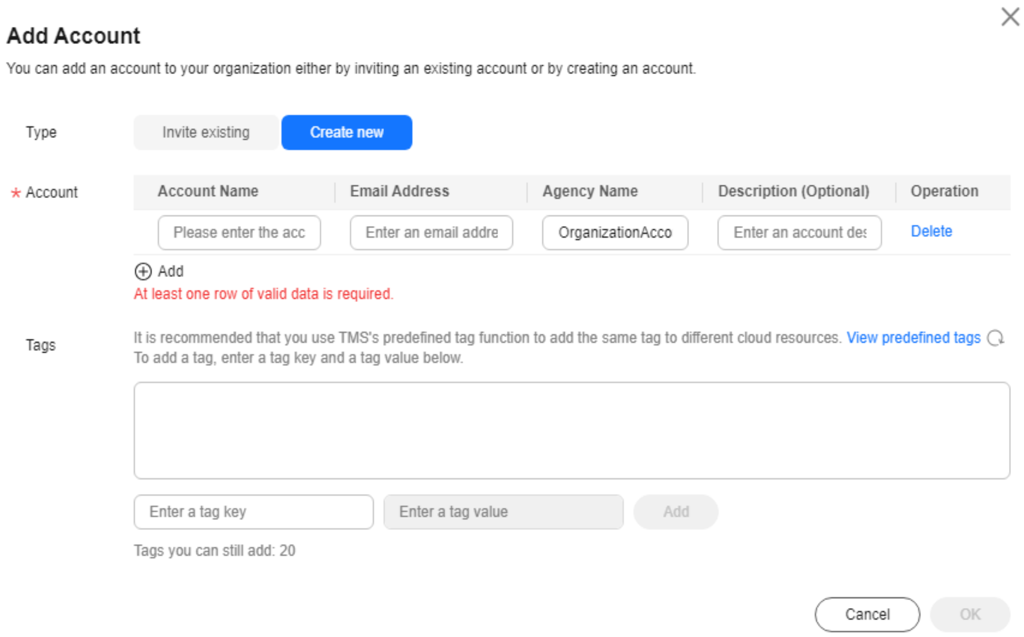


**Step 3** Click **Create new** in the displayed dialog box.

**Step 4** Enter the account name and email address. Ensure that the account name is different from any existing one.

You can retain the default agency name or change it as required.

**Figure 4-6** Creating an account



Add Account

You can add an account to your organization either by inviting an existing account or by creating an account.

Type: Invite existing | Create new

* Account

| Account Name | Email Address | Agency Name | Description (Optional) | Operation |
|---|---|---|---|---|
| Please enter the acc | Enter an email addre | OrganizationAcco | Enter an account des | Delete |

At least one row of valid data is required.

Tags

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags
To add a tag, enter a tag key and a tag value below.

Tags you can still add: 20

**Step 5** (Optional) Add one or more tags to the account.

A tag consists of a key-value pair. Tags are used to identify, classify, and search for accounts. You can add up to 20 tags to an account.

Table 4-3 describes the key and value descriptions of a tag.

**Table 4-3** Tag description

| Element | Description | Example |
|---|---|---|
| Tag key | A tag key of an account must be unique. You can create a custom key or select a key of an existing tag created in Tag Management Service (TMS).<br>A tag key:<br>● Cannot be an empty string.<br>● Contains 1 to 128 characters.<br>● Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF). | Key_0001 |
| Tag value | A tag value can be repetitive or an empty string.<br>A tag value:<br>● Can be an empty string.<br>● Contains 1 to 225 characters.<br>● Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF). | Value_0001 |

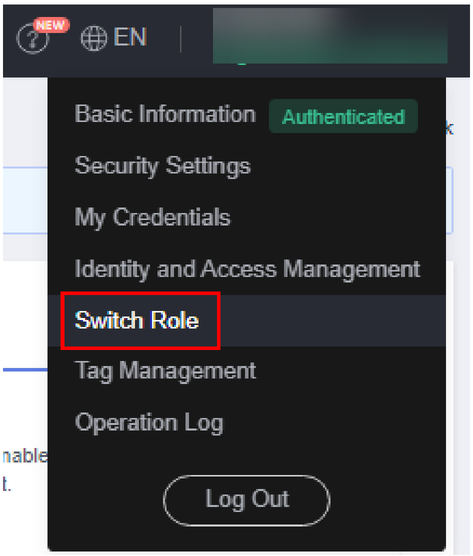
**Step 6** Click **OK**. The new account is added to the list.

**----End**

## Accessing Account Resources Via Agency

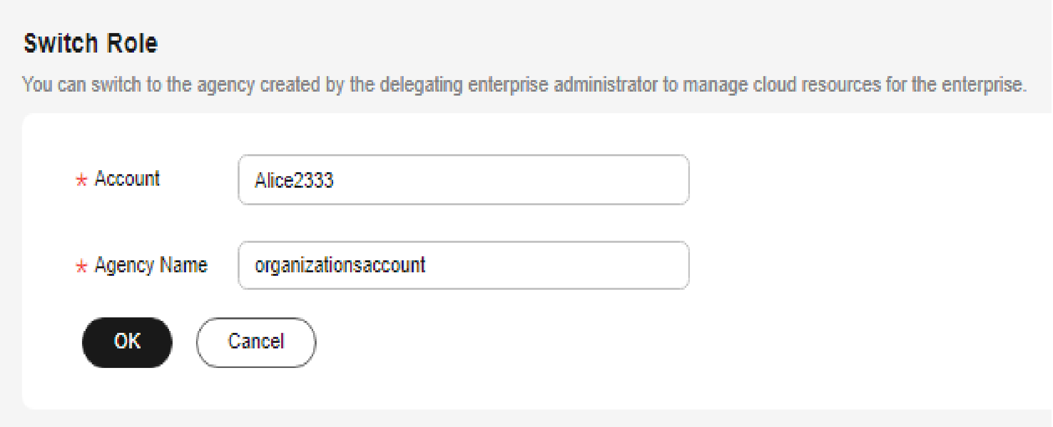
**Step 1** Hover the mouse pointer over the username in the upper right corner and choose **Switch Role**.

**Figure 4-7** Switching the role



**Step 2** On the **Switch Role** page, enter the account name.

**Figure 4-8** Entering the account name



Switch Role

You can switch to the agency created by the delegating enterprise administrator to manage cloud resources for the enterprise.

* Account: Alice2333

* Agency Name: organizationsaccount

NOTE

After you enter the account name, the agencies created under this account will be automatically displayed when you click the agency name text box. An agency name starting with **cbc_** will also be displayed. This agency is mainly used by an enterprise master account to centrally manage expenditures and grant permissions to member accounts. You need to select the agency name entered when creating the account.

**Step 3** Click **OK** to switch to the account.

**----End**

### Accessing Account Resources Via IAM Identity Center

You can associate an account with users and permission sets in IAM Identity Center, and log in to the IAM Identity Center console via the user portal URL to access the resources in the account in the given organization. The specific access permission for resources is controlled by the permission set in IAM Identity Center.

## 4.4 Closing an Account

If you no longer need a member account, you can close it from the management account of your organization following the instructions in this section. If you want to close the management account, you have to delete your organization. For details, see **Deleting an Organization**.

CAUTION

- Once your request to close an account is submitted, data in the account will start to be deleted and cannot be restored. This operation cannot be undone.
- After the data in an account is deleted, the account status changes to **Closed**. The account will be retained in the account list for 90 days before being permanently deregistered.

## Constraints

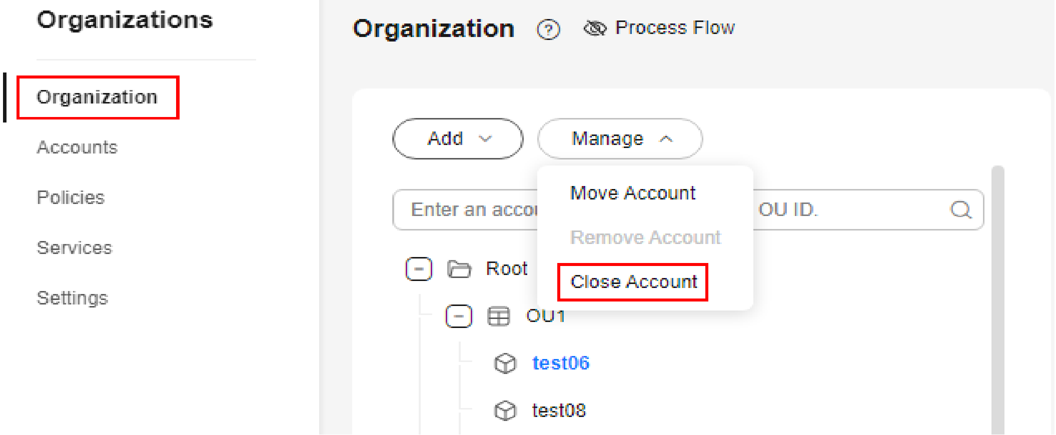
- You can close accounts you created but not those you invited to your organization.
- If any accounts you created have become cloud accounts, they cannot be closed.
- Any account that is specified as a delegated administrator cannot be closed unless you remove the delegated administrator first, as described in **Removing a Delegated Administrator**.
- The management account can only close 10% of the member accounts (no more than 200 accounts) in a given organization within 30 days, and no more than three at a time.
- The mobile number or email address associated with the closing account cannot be used to create another account.
- Any account that has prepaid resources, generally yearly/monthly resources, cannot be closed unless you confirm and unsubscribe from such resources, as described in **Unsubscribing from In-Use Resources**.
- Any account that has resources in arrears cannot be closed unless you top up your account and pay off the arrears, as described in **Top-Up and Payment**.

## Procedure

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the account you want to close and choose **Manage** > **Close Account**.

**Figure 4-9** Closing an account



**Step 3** In the displayed dialog box, read and confirm the risks of closing the account, and enter the account name to reconfirm the operation.

**Step 4** Click **OK**.

**----End**

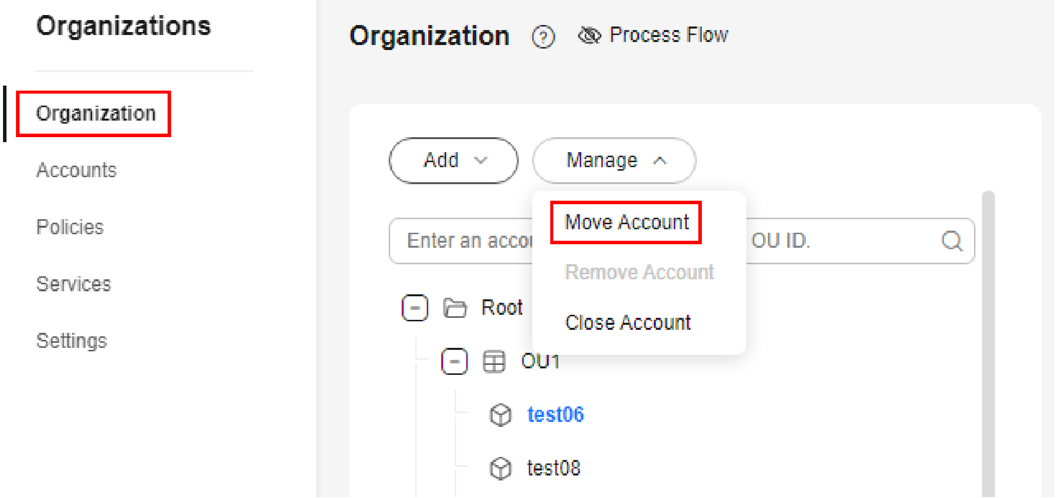
## 4.5 Moving an Account

When you log in as the management account, you can move an account from one OU to another.

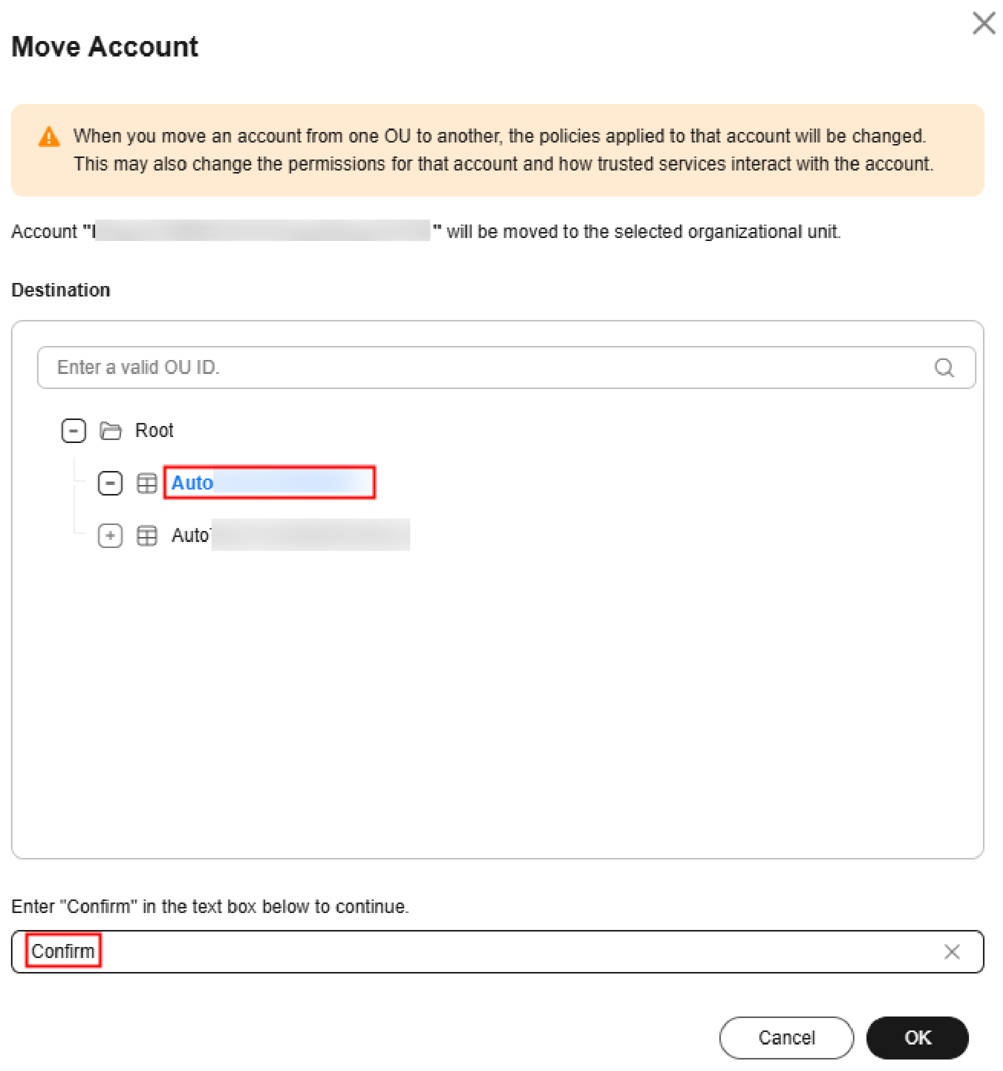
**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the account you want to move, and choose **Manage** > **Move Account**.

**Figure 4-10** Moving an account



**Step 3** Select the OU you choose to hold the account, and enter "Confirm" in the text box. Then, click **OK**.



Move Account

When you move an account from one OU to another, the policies applied to that account will be changed. This may also change the permissions for that account and how trusted services interact with the account.

Account "I[redacted]" will be moved to the selected organizational unit.

Destination

Enter a valid OU ID.

Enter "Confirm" in the text box below to continue.

Confirm

**----End**

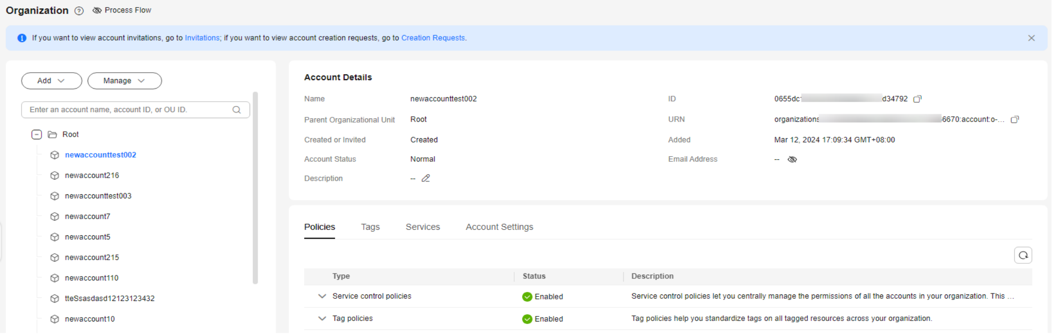
# 4.6 Viewing Account Details

You can view the details of accounts in your organization at any time by following the steps below.

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the account you want to view. Its details are displayed in the pane on the right, including the account name, ID, home OU, URN, how and when the account joined the organization, when the account was created, account status, email address, account description, as well as policies, tags, and deleted services.

**Figure 4-11** Viewing account details



If you want to view account invitations, go to Invitations; if you want to view account creation requests, go to Creation Requests.

Account Details

Name: newaccounttest002
Parent Organizational Unit: Root
Created or Invited: Created
Account Status: Normal
Description: --
ID: 0655dc[redacted]d34792
URN: organizations[redacted]6670:account:o-...
Added: Mar 12, 2024 17:09:34 GMT+08:00
Email Address: --

| Type | Status | Description |
|---|---|---|
| Service control policies | Enabled | Service control policies let you centrally manage the permissions of all the accounts in your organization. This ... |
| Tag policies | Enabled | Tag policies help you standardize tags on all tagged resources across your organization. |

**----End**

# 4.7 Removing a Member Account from Your Organization

## Precautions

Before the organization administrator removes a member account from an organization or before a member account leaves an organization, it is important to know the following:

- The member account in question has to have been created more than seven calendar days ago.
- The account has to have been converted to a Huawei Cloud account.
- Only Huawei Cloud accounts can be removed from an organization or leaves an organization.
- A delegated administrator account cannot be removed from or leave an organization. You need to remove the delegated administrator first. For details, see **Removing a Delegated Administrator**.
- After an account created via Organizations leaves an organization, the IAM agency created by default during the creation of the account will not be automatically deleted. The organization management account can still use that agency to access data of member accounts. To prevent unauthorized access, you need to manually delete the agency. For details, see **Deleting an Agency**.
- After an account created via Organizations leaves the organization, the accounting relationship between the account and the organization management account remains unchanged. After an account that was invited to join an organization leaves the organization, its original accounting relationship remains unchanged. For details about how to disassociate a member account, see **Disassociating Member Accounts**.
- After a member account leaves an organization, the permissions assigned by the organization policies will no longer apply. This means that the account may actually have more permissions than before. If you enabled trusted access for a cloud service, the account can no longer use the functions of that trusted service.

- When a member account leaves an organization, all tags attached to the account are deleted.

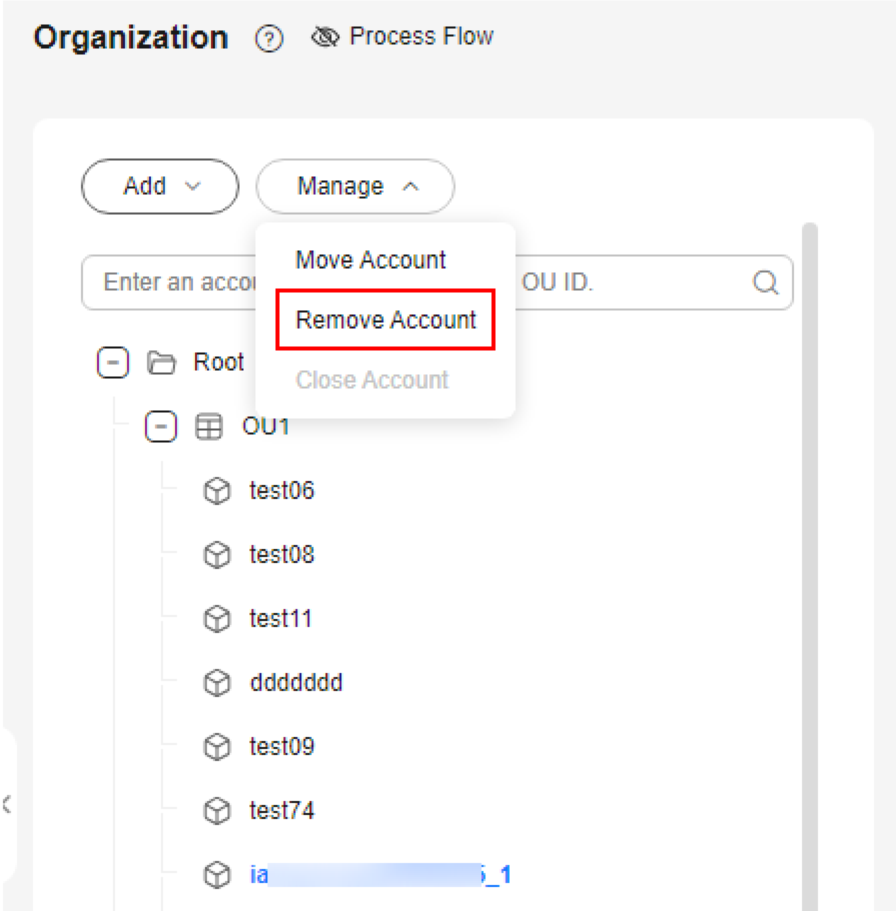
## Removing an Account

When you sign in to the management account of your organization, you can remove member accounts that you no longer need. The following steps apply only when you remove member accounts. If you want to remove the management account, you must delete the organization by following the instructions in **Deleting an Organization**.

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

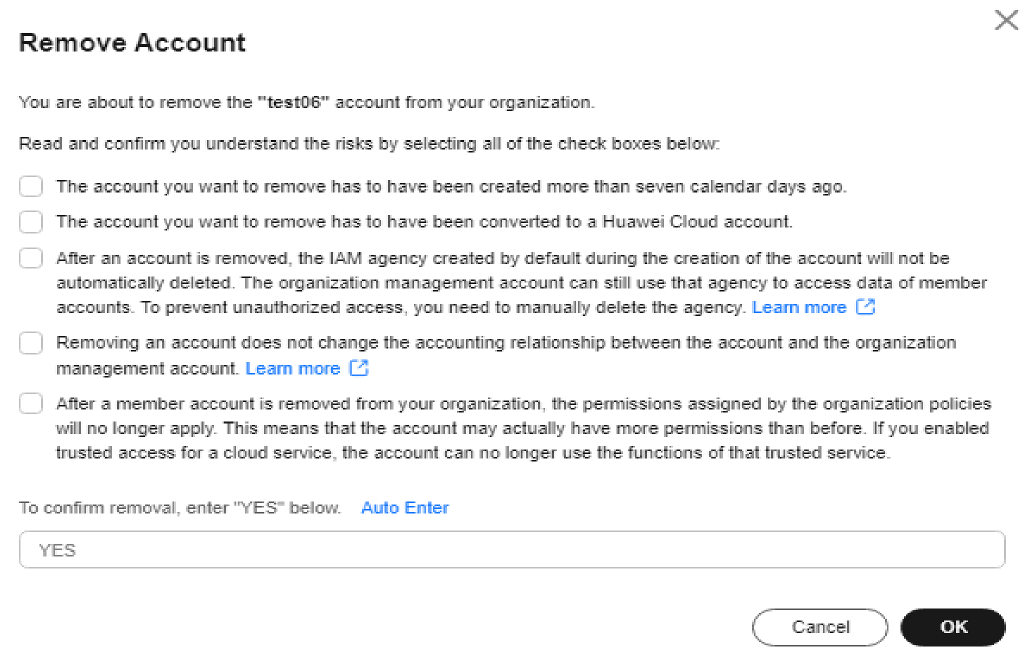
**Step 2** Select the account you want to remove, and choose **Manage** > **Remove Account**.

**Figure 4-12** Removing an account



**Step 3** In the displayed dialog box, read and confirm you understand the risks by selecting all of the check boxes, and then enter **YES** and click **OK**.

**Figure 4-13** Confirming the risks of removing the account



Remove Account

You are about to remove the **"test06"** account from your organization.

Read and confirm you understand the risks by selecting all of the check boxes below:

□ The account you want to remove has to have been created more than seven calendar days ago.

□ The account you want to remove has to have been converted to a Huawei Cloud account.

□ After an account is removed, the IAM agency created by default during the creation of the account will not be automatically deleted. The organization management account can still use that agency to access data of member accounts. To prevent unauthorized access, you need to manually delete the agency. Learn more

□ Removing an account does not change the accounting relationship between the account and the organization management account. Learn more

□ After a member account is removed from your organization, the permissions assigned by the organization policies will no longer apply. This means that the account may actually have more permissions than before. If you enabled trusted access for a cloud service, the account can no longer use the functions of that trusted service.

To confirm removal, enter "YES" below. Auto Enter

YES

**----End**

## Leaving an Organization As a Member Account

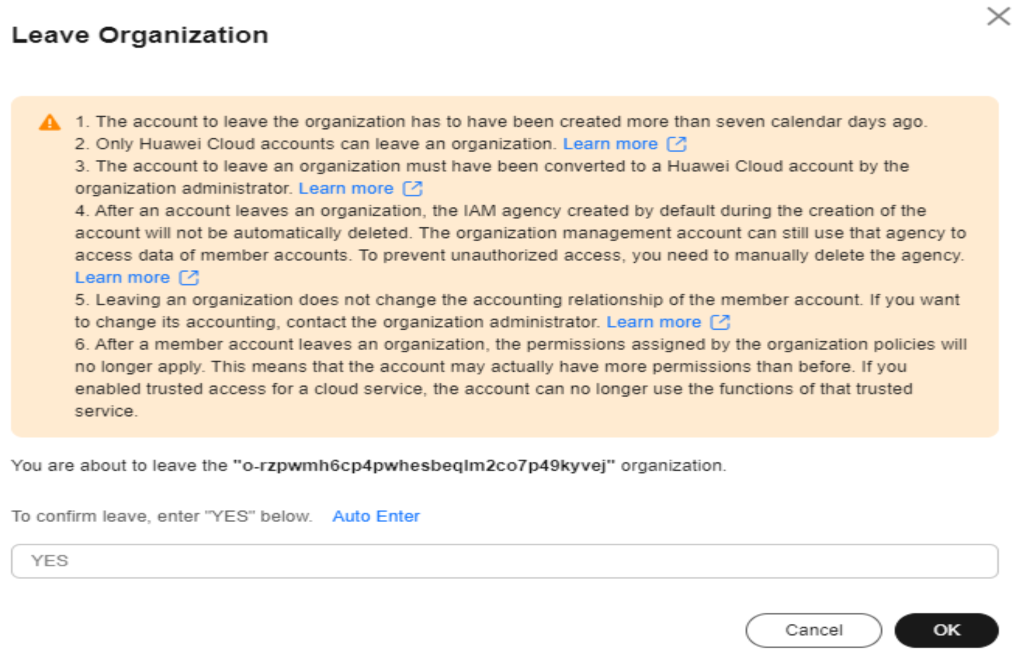
When you sign in to a member account of an organization, you can choose to leave the organization. The management account cannot leave the organization using this method. To remove the management account, you must delete the organization by referring to **Deleting an Organization**.

Any account that is specified as a delegated administrator cannot leave an organization unless you remove the delegated administrator first, as described in **Removing a Delegated Administrator**.

**Step 1** Log in to Huawei Cloud as a member account, and navigate to the Organizations console.

**Step 2** On the **Settings** page, click **Leave Organization**. In the displayed dialog box, read and confirm you understand the risks, and then enter **YES** and click **OK**.

**Figure 4-14** Confirming the risks of leaving the organization



Leave Organization

1. The account to leave the organization has to have been created more than seven calendar days ago.
2. Only Huawei Cloud accounts can leave an organization. Learn more
3. The account to leave an organization must have been converted to a Huawei Cloud account by the organization administrator. Learn more
4. After an account leaves an organization, the IAM agency created by default during the creation of the account will not be automatically deleted. The organization management account can still use that agency to access data of member accounts. To prevent unauthorized access, you need to manually delete the agency. Learn more
5. Leaving an organization does not change the accounting relationship of the member account. If you want to change its accounting, contact the organization administrator. Learn more
6. After a member account leaves an organization, the permissions assigned by the organization policies will no longer apply. This means that the account may actually have more permissions than before. If you enabled trusted access for a cloud service, the account can no longer use the functions of that trusted service.

You are about to leave the **"o-rzpwmh6cp4pwhesbeqlm2co7p49kyvej"** organization.

To confirm leave, enter "YES" below. Auto Enter

YES

**----End**

# 4.8 Viewing Account Invitation/Creation Records

When you sign in to the management account of your organization, on the **Accounts** page, you can view account details, including the account list, creation records, and invitations. You can also invite, create, close, move, and remove accounts and cancel any pending invitations.

This section includes the following content:

- **Viewing the Account List**
- **Viewing Invitations**
- **Viewing Creation Requests**

## Viewing the Account List

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** Access the **Accounts** page, and click the **Accounts** tab.

In the account list, you can view the details of all the accounts in your organization.

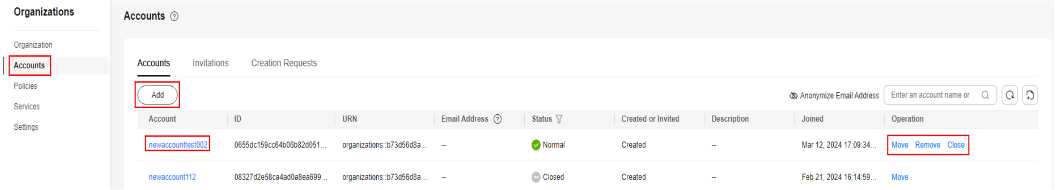
**Step 3** Click an account name in the list to view its details.

**Step 4** Click **Move**, **Close**, or **Remove** in the **Operation** column.

You cannot close any accounts that have been invited to your organization.

**Step 5** Click **Add** in the upper left corner of the list. In the displayed dialog box, you can invite existing accounts to join your organization or create new accounts in the organization.

**Figure 4-15** Account list



| Account | ID | URN | Email Address | Status | Created or Invited | Description | Joined | Operation |
|---|---|---|---|---|---|---|---|---|
| newaccounttest002 | 0655dc159cc64b06b82d051... | organizations::b73d56d8a... | -- | Normal | Created | -- | Mar 12, 2024 17:09:34... | Move Remove Close |
| newaccount112 | 08327d2e58ca4ad0a8ea699... | organizations::b73d56d8a... | -- | Closed | Created | -- | Feb 21, 2024 16:14:59... | Move |

**----End**

## Viewing Invitations

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

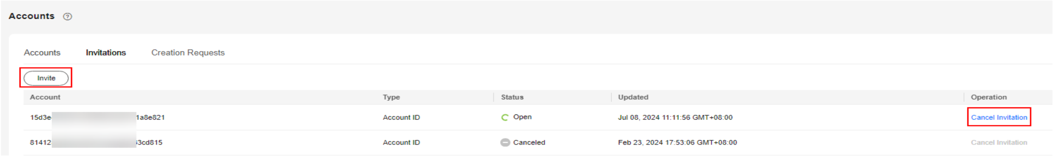
**Step 2** On the **Accounts** page, click the **Invitations** tab.

You can view the details about account invitations.

**Step 3** Click **Cancel Invitation** in the **Operation** column to cancel an invitation in the **Open** state.

**Step 4** Click **Invite** in the upper left corner of the list. In the displayed dialog box, you can invite existing accounts to join your organization.

**Figure 4-16** Invitations



| Account | Type | Status | Updated | Operation |
|---|---|---|---|---|
| 15d3e[redacted]1a8e821 | Account ID | Open | Jul 08, 2024 11:11:56 GMT+08:00 | Cancel Invitation |
| 81412[redacted]3cd815 | Account ID | Canceled | Feb 23, 2024 17:53:06 GMT+08:00 | Cancel Invitation |

**----End**

## Viewing Creation Requests

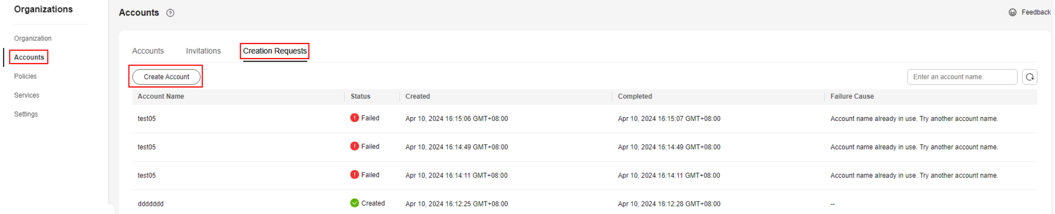
**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Accounts** page, click the **Creation Requests** tab.

You can view the details about account creation requests.

**Step 3** Click **Create Account** in the upper left corner of the list. In the displayed dialog box, you can create new accounts for your organization.

**Figure 4-17** Creation requests



| Account Name | Status | Created | Completed | Failure Cause |
|---|---|---|---|---|
| test05 | ● Failed | Apr 10, 2024 16:15:06 GMT+08:00 | Apr 10, 2024 16:15:07 GMT+08:00 | Account name already in use. Try another account name. |
| test05 | ● Failed | Apr 10, 2024 16:14:49 GMT+08:00 | Apr 10, 2024 16:14:49 GMT+08:00 | Account name already in use. Try another account name. |
| test05 | ● Failed | Apr 10, 2024 16:14:11 GMT+08:00 | Apr 10, 2024 16:14:11 GMT+08:00 | Account name already in use. Try another account name. |
| ddddddd | ✓ Created | Apr 10, 2024 16:12:25 GMT+08:00 | Apr 10, 2024 16:12:28 GMT+08:00 | -- |

**----End**

# 5 Managing SCPs

## 5.1 Overview of an SCP

### 5.1.1 SCP Introduction

#### What Are Service Control Policies?

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. The organization management account can use SCPs to limit which permissions can be assigned to member accounts to ensure that they stay within your organization's access control guidelines. SCPs can be attached to an organization, OUs, and member accounts. Any SCP attached to an organization or OU affects all the accounts within the organization or under the OU.

Helpful links:

- **SCP Principles**: SCP types, how SCPs work, inheritance of SCPs, and relationship between SCPs and IAM policies
- **SCP Syntax**: SCP structure and parameters

#### Testing SCP Effects

Before applying an SCP to your production environment, it is strongly recommended that you use test accounts in a test environment first to perform thorough system design and testing. This helps avoid any unpleasant surprises in the production environment. After the SCP has been fully verified in the test environment, you can create an OU and move one or a few accounts into it at a time, to ensure that the use of resources is not inadvertently interrupted.

⚠ CAUTION

Do not detach the system-defined SCP **FullAccess** unless you replace it with a custom policy with allowed actions. **If you detach FullAccess and configure a custom policy with allowed actions, you must configure actions required by services as well as iamToken::* and signin::*.**

- If you detach the FullAccess SCP from the root OU, the operations for all accounts in the organization will fail. Exercise caution when detaching the FullAccess SCP because this operation is very risky.
- If you detach the FullAccess SCP from an OU, the operations for the accounts in that OU and its lower-level OUs will fail.
- If you detach the FullAccess SCP from a member account, the operations for that account will fail.

## Tasks Not Restricted by SCPs

You cannot use SCPs to restrict the following tasks:

- Any actions performed by the organization management account or IAM users.
- Any actions performed using permissions that are attached to a service-linked agency.
- Any API calls made by SCP-unsupported cloud services to SCP-supported cloud services. For SCP-supported cloud services and regions, see **Cloud Services for Using SCPs** and **Regions for Using SCPs**.
- **Token obtained by APIs** used for access to APIs of SCP-supported cloud services (in most cases).

## Helpful Links

For details about the differences in access control between IAM and Organizations, see **What Are the Differences in Access Control Between IAM and Organizations?**

# 5.1.2 SCP Principles

## SCP Types

SCPs are classified as either system-defined policies or custom policies, depending on who creates them.

- **System-defined policies**

System-defined policies refer to commonly used SCPs predefined by Huawei Cloud services for Organizations. An organization administrator can directly use these policies when attaching SCPs to OUs or accounts. Such policies cannot be modified. For details about available SCP system policies, see **System-defined SCPs**.

- **Custom policies**

If system-defined policies cannot meet your requirements, you can use the management account to create and modify custom SCPs based on the actions supported by each service. Custom policies extend and supplement system-defined policies. You can create custom policies for Organizations in a policy editor or JSON view.

## SCP Effects on Permissions

- **Permissions boundaries**

  SCPs do not actually grant any permissions to an entity. They only set permissions boundaries for the entity. When SCPs are attached to an OU or a member account, they do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs. Users cannot perform any actions that are denied by SCPs even if the actions are granted to the users by IAM policies.

  Suppose that an SCP is attached to a member account. The SCP allows action A but denies action B. The member account then can grant its IAM users the permission to perform action A but not action B. Even if the permission to perform action B is assigned, the permission cannot be applied.

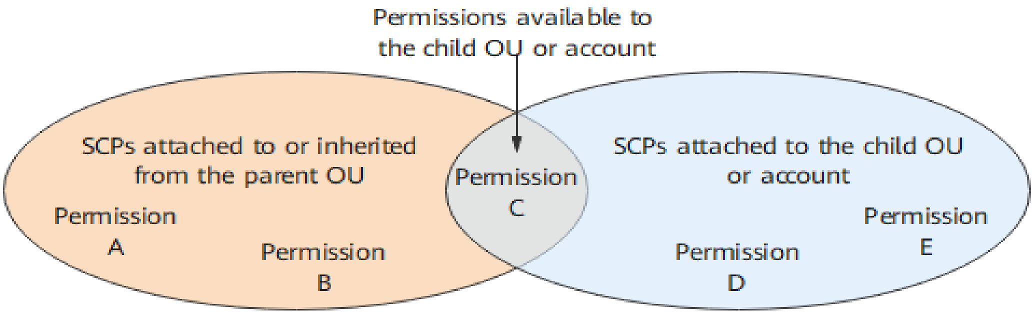
- **Permissions intersection**

  The final effective permissions of an OU or account are the intersection of the permissions of its own SCPs and the allowed SCPs of its parent OU.

  In the following figure, the oval on the left represents an SCP attached to the parent OU. It allows permissions A, B, and C. The oval on the right represents an SCP attached to the child OU or account. It allows permissions C, D, and E. Because the SCP attached to the parent OU does not allow permission D or E, no child OUs or accounts under the parent OU can use them. Even though the SCP attached to the child OU explicitly allows permissions D and E, they are blocked by the SCP attached to the parent OU. Because the SCP attached to the child OU or account does not allow permission A or B, those permissions are blocked for the child OU or account. In this case, the child OU or account can actually use the permission (permission C in the following figure) in the intersection of its own permissions and the allowed permissions of its parent OU.

  If the entity in the set on the right represents a member account, the set of maximum permissions that can be granted to the users and user groups in that account is the intersection of the two sets. If the entity represents a child OU, then the set of maximum permissions that can be granted to that OU is the intersection of the two sets.

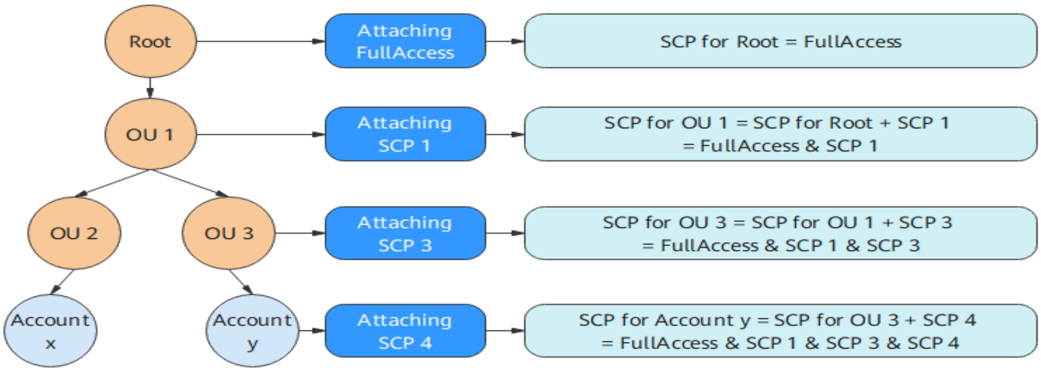
**Figure 5-1** How SCPs work


Permissions available to the child OU or account
SCPs attached to or inherited from the parent OU
Permission A
Permission B
Permission C
SCPs attached to the child OU or account
Permission D
Permission E

- **Policy inheritance**

  SCPs for an OU or account can be attached directly or inherited from the root OU or the parent OU. When you attach an SCP to a specific OU, all child OUs and accounts under that OU will inherit that policy. The permissions boundaries of an account or an OU are determined by a combination of the SCPs attached to all upper-level OUs and the SCPs directly attached to the account or OU. In the following figure, Account y is nested in OU 3, and its permissions boundary is jointly determined by the SCPs inherited from the root OU and the SCPs attached to OU 1 and OU 3 as well as Account y.

  **Figure 5-2** Example SCP inheritance

  
  Root
OU 1
OU 2
OU 3
Account x
Account y
Attaching FullAccess
Attaching SCP 1
Attaching SCP 3
Attaching SCP 4
SCP for Root = FullAccess
SCP for OU 1 = SCP for Root + SCP 1 = FullAccess & SCP 1
SCP for OU 3 = SCP for OU 1 + SCP 3 = FullAccess & SCP 1 & SCP 3
SCP for Account y = SCP for OU 3 + SCP 4 = FullAccess & SCP 1 & SCP 3 & SCP 4

  If you want to allow a service action at the member account level, you must allow that action at every level between the member account and the root OU of your organization. Specifically, you must attach SCPs that allow the given action to every level from the root OU to the member account. You can use either a deny list or an allow list.

  A deny list: This strategy uses the **FullAccess** SCP that is attached by default to every OU and account. This SCP overrides the default implicit Deny and allows all permissions to flow down from the root OU to every account, unless you explicitly deny a permission with an additional SCP that you create and attach to the appropriate OU or account. No account below the level of the OU with the deny policy can use the denied action, and there is no way to add the permission back lower in the hierarchy.

- **Allow by default**

  When SCPs are enabled for an organization, the **FullAccess** policy is attached by default to all OUs and accounts unless you attach explicit deny policies to the OUs or accounts.

## Differences Between Explicit Deny and Implicit Deny

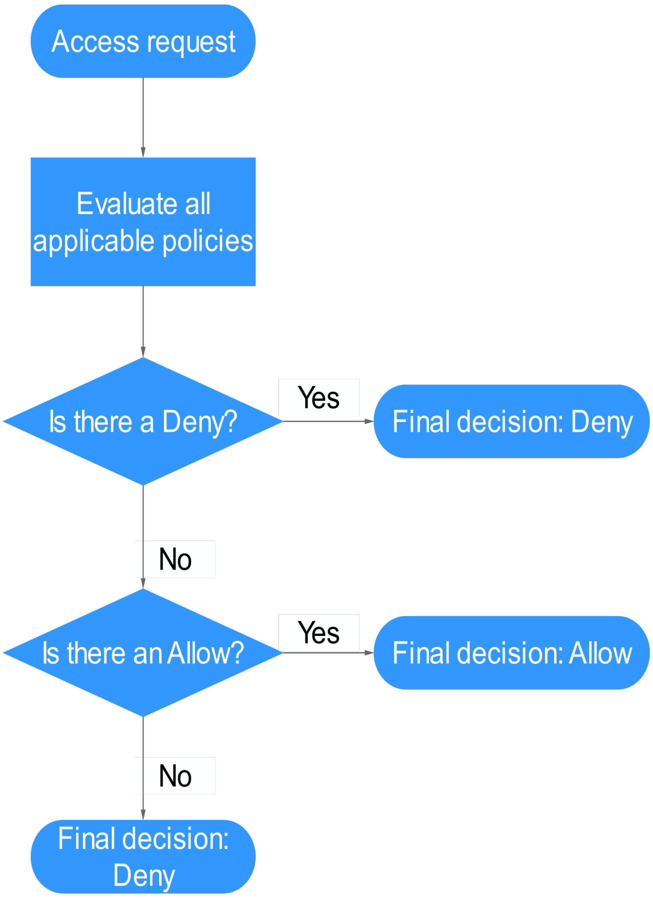
The effect of Deny indicates the permission to deny an operation.

If there are no applicable Deny statements, all requests are denied by default. This is called an implicit deny.

If a policy includes an applicable Deny statement, requests will be denied. This is called an explicit deny.

The following figure shows the logic for authenticating an access request.

**Figure 5-3** Authentication logic



1. A principal sends an access request.
2. The system looks for a Deny statement that applies to the request. If the system finds an applicable Deny, it returns a final decision of Deny, and the authentication ends.
3. If no applicable Deny is found, the system looks for an Allow that would apply to the request. If the system finds an applicable Allow, it returns a final decision of Allow, and the authentication ends.
4. If no applicable Allow is found, the system returns a final decision of Deny, and the authentication ends.

## 5.1.3 SCP Syntax

The following uses a custom policy for RAM as an example to describe the SCP syntax.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
       "ForAnyValue:StringNotEquals": {
          "g:RequestTag/owner": [
            "Alice",
            "Jack"
          ]
        }
      }
    }
  ]
}
```

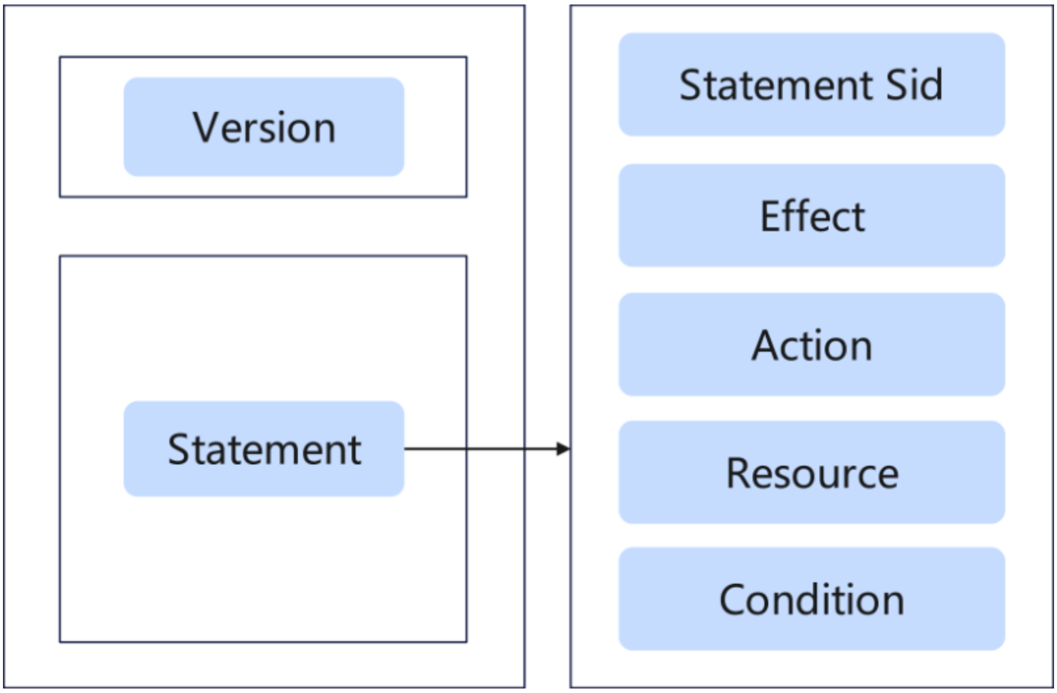
NOTE

SCPs use a similar syntax to that used by IAM identity policies.

### Policy Structure

A policy consists of a version and a single statement or an array of individual statements, each indicating a different action.

**Figure 5-4** Policy structure



## Policy Elements

The following table describes the policy elements (**Version** and **Statement**).

**Table 5-1** Policy elements

| Element | | Mandatory | Description | Value |
|---|---|---|---|---|
| Version | | Yes | Policy version. | 5.0 (cannot be customized) |
| Statement:<br>Permissions defined by a policy | Statement ID (Sid) | No | Identifier of a policy statement. You can assign a Sid value for each statement in a statement array. | A user-defined character string |
| | Effect | Yes | Determines whether to allow or deny the operations defined in an action. | • **Deny** |
| | Action | Optional for Deny statements | Operations that the SCP allows or denies. | Format: "*Service name*:*Resource type*:*Operation*".<br>For example, **vpc:subnets:list** indicates the permission to view the VPC subnet list, where **vpc** is the service name, **subnets** refers to the resource type, and **list** is the action. |
| | | | | |
| | Condition | Optional for Deny statements | Determines when a policy is in effect. A condition consists of a **condition key** and a **condition operator**. | Format: "*Condition operator*:{*Condition key*:[*Value 1*,*Value 2*]}"<br>If you configure multiple conditions, the policy can be applied only when all the conditions are met.<br>Example:<br>**"StringEndWithIfExists":{"g:UserName":["specialCharactor"]}**: This statement is valid for users whose names end with **specialCharactor**. |

| Element | | Mandatory | Description | Value |
|---|---|---|---|---|
| | Resource | No<br>If this element is not specified, * is used by default, indicating that the SCP applies to all resources. | Resources that the SCP applies to. | The value can be either * or a specific resource for Deny statements. Format: *Service name*:region:domain ID:*Resource type*:*Resource path*. Wildcard characters (*) are supported, indicating all resources.<br>Example: "ecs:*:*:instance:*", representing all ECS instances. |

NOTE

The following elements are not supported in SCPs:

- Principal
- NotPrincipal
- NotResource
- NotAction

## Condition Keys

A condition key is a key in the **Condition** element of a statement. The condition key that you specify can be a global condition key or a service-specific condition key.

- Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, Organizations automatically obtains user information and authenticates users.
- Service-specific condition keys (with the abbreviation of a service name as the prefix, for example, **ram:**) apply only to operations of that service.

**Table 5-2** Common global condition keys

| Global Condition Key | Type | Description |
|---|---|---|
| g:CalledVia | String array | Used to control access across services. When a principal initiates an access request to a cloud service, the service may forward the request to another service. The g:CalledVia key contains a list of services in the chain that send requests on behalf of the principal. This condition key is present when the service forwards the access request of the principal. This condition key is not present when the principal accesses the service directly. See an example in 1. |
| g:CalledViaFirst | String | Similar to g:CalledVia, it refers to the first element in the g:CalledVia key, which means the first service that forwards a request on behalf of the principal. |
| g:CalledViaLast | String | Similar to g:CalledVia, it refers to the last element in the g:CalledVia key, which means the last service that forwards a request on behalf of the principal. |
| g:CurrentTime | Time | Time when a request is received. It is in ISO 8601 format, for example, 2012-11-11T23:59:59Z. See an example in 2. |
| g:DomainName | String | Account name of the requester. |
| g:DomainId | String | Account ID of the requester. |
| g:EnterpriseProjectId | String | ID of the enterprise project for the request or the requested resource. This condition key is present when the ID of the enterprise project for the request or the requested resource is passed in the API request and the action supports g:EnterpriseProjectId. This condition key is used in authentication, rather than a filter condition. This means resources in the enterprise project specified by this condition key will not be filtered out. See an example in 3. |
| g:MFAPresent | Boolean | Whether to use multi-factor authentication (MFA) to obtain STS security tokens. This condition key is true only when you log in to the console through MFA or when you use the assumed-agency session obtained through MFA to make a request. This condition key is present only when a request is sent using STS Security Token. See an example in 4. |

| Global Condition Key | Type | Description |
|---|---|---|
| g:MFAAge | Numeric | Validity period of STS security tokens obtained through MFA authentication. This condition key is present only when you log in to the console through MFA authentication or when you use the assumed-agency session obtained through MFA to make a request. The unit is second. |
| g:PrincipalAccount | String | Same as g:DomainId. |
| g:PrincipalUrn | String | URN of the requesting principal. Different principals have different URN formats.<br>IAM users: iam::<domain-id>:user:<user-name><br>IAM assumed-agency sessions: sts::<domain-id>:assumed-agency:<agency-name>/<session-name><br>Virtual federated users: sts::<domain-id>:external-user:<idp-id>/<session-name><br>See an example in **5**. |
| g:PrincipalIsRootUser | Boolean | Whether the requesting principal is an IAM root user. This condition key is present in all requests. |
| g:PrincipalIsService | Boolean | Whether the requesting principal is a cloud service. You can use this condition key to control whether only cloud services can access the specified APIs. |
| g:PrincipalOrgId | String | ID of the organization that the requesting principal belongs to. You can use this condition key to control access to the specified APIs only from identities in the specific organization. This condition key is present only when the requesting principal is part of an organization. See an example in **6**. |
| g:PrincipalOrgManagementAccountId | String | ID of the management account in the organization that the requesting principal belongs to. This condition key is present only when the requesting principal is part of an organization. See an example in **7**. |

| Global Condition Key | Type | Description |
|---|---|---|
| g:PrincipalOrgPath | String | Path of the organization that the requesting principal belongs to. You can use this condition key to control access to the specified APIs only from accounts within the specified organization root or organizational units (OUs). This condition key is present only when the requesting principal is part of an organization. See an example in **8**.<br>An account's organization path is in the following format:<br><organization-id>/<root-id>/(<ou-id>/)*<account-id> |
| g:PrincipalServiceName | String | Requesting principal's name. This condition key is present only when the requesting principal is a cloud service. See an example in **9**. |
| g:PrincipalTag/<tag-key> | String | Tag contained in the requesting principal. The <tag-key> is case insensitive. This condition key is present only when the requesting principal is a tagged IAM user or trust agency, or an assumed-agency session with a session tag. See an example in **10**. |
| g:PrincipalType | String | Type of the requesting principal, which can be **User**, **AssumedAgency**, or **ExternalUser**. When an IAM user is used for access, the value is **User**. When an IAM assumed-agency session is used for access, the value is **AssumedAgency**. When a virtual federated user is used for access, the value is **ExternalUser**. |
| g:Referer | String | HTTP referer header in a request. As this condition key is specified by the client, it should not be used to prevent unauthorized access. |
| g:RequestedRegion | String | Region called in a request. If the requested cloud service is a region-specific service, set this condition key to the corresponding region ID, for example, cn-north-4. This condition key is present only when certain region-specific services are requested. |
| g:RequestTag/<tag-key> | String | Tag contained in a request. The <tag-key> is case insensitive. If a requester passes a tag when calling an API (for example, for adding a tag to an existing resource, or adding a tag during resource creation), you can use this condition key to check whether the request contains the tag. This condition key is present only when the action supports g:RequestTag/<tag-key> and tags are passed in the API request. See an example in **11**. |

| Global Condition Key | Type | Description |
|---|---|---|
| g:ResourceAccount | String | Requested resource owner's account ID. This condition key is present only in actions of cloud services that support fine-grained permissions management. See an example in **12**. |
| g:ResourceOrgId | String | ID of the organization that the requested resource account belongs to. This condition key is present only in actions of cloud services that support fine-grained permissions management and the resource owner account is part of an organization. See an example in **13**. |
| g:ResourceOrgPath | String | Path in the organization that the requested resource account belongs to. This condition key is present only in actions of cloud services that support fine-grained permissions management and the resource owner account is part of an organization. See an example in **14**. |
| g:ResourceTag/<tag-key> | String | Tag contained in the requested resource. The tag key <tag-key> is case insensitive. You can use this condition key to control that only resources with specified tags attached can be accessed. This condition key is present only when the action supports g:ResourceTag/<tag-key> and tags are attached to the requested resources. See an example in **15**. |
| g:SecureTransport | Boolean | Whether the request is sent using SSL. |
| g:SourceAccount | String | Account of the resource making a service-to-service request in cross-service access scenarios. This condition key is present only when the action supports g:SourceAccount. It should only be used in resource policies where the cloud service is the principal. See an example in **16**. |
| g:SourceUrn | String | URN of the resource making a service-to-service request. This condition key is present only when the action supports g:SourceUrn. It should only be used in resource policies where the cloud service is the principal. See an example in **17**. |
| g:SourceIdentity | String | The **source_identity** field specified when a user obtains IAM temporary credentials through the AssumeAgency API of STS for the first time. This field cannot be changed during subsequent agency switches. This condition key is present only when a request with **source_identity** specified is sent using STS Security Token. See an example in **18**. |

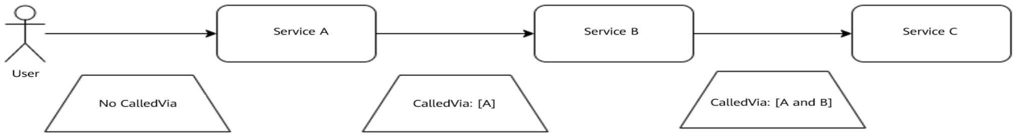
| Global Condition Key | Type | Description |
|---|---|---|
| g:SourceIp | IP | Source IP address from a public network. See an example in **19**.<br>**NOTE**<br>If the request is initiated within a VPC and passes through a VPC endpoint, g:VpcSourceIp would be used instead of g:SourceIp. This condition key is present only if the access is not initiated through a VPC endpoint. This condition key can be used as a valid access control condition only when the access is initiated through a public network. It does not take effect when a cloud service uses an agency to initiate access on behalf of a user without going through a public network. |
| g:SourceVpc | String | ID of the VPC from which the request is sent. This condition key is present only when the request is initiated within a VPC and passes through a VPC endpoint to access a cloud service that is configured as a VPC endpoint service. |
| g:SourceVpce | String | ID of the VPC endpoint that initiates the request. This condition key is present only when the request is initiated within a VPC and passes through a VPC endpoint to access a cloud service that is configured as a VPC endpoint service. See an example in **20**. |
| g:TagKeys | String array | List of tag keys in a request. This condition key is present only when the action supports g:TagKeys and tags are passed in the API request. |
| g:TokenIssueTime | Time | Time when STS Security Token in the access credentials is issued. This condition key is present only when a request is sent using STS Security Token. |
| g:UserAgent | String | HTTP User-Agent header in a request. As this condition key is specified by the client, it should not be used to prevent unauthorized access. |
| g:PrincipalId | String | ID of the requesting principal. Different principals have different ID formats.<br>IAM users: <user-id><br>IAM assumed-agency sessions: <agency-id>:<session-name><br>Virtual federated users: <idp-id>:<session-name> |
| g:UserName | String | Name of an IAM user. This condition key is present only when the requester is an IAM user. |
| g:UserId | String | ID of an IAM user. This condition key is present only when the requester is an IAM user. |

| Global Condition Key | Type | Description |
|---|---|---|
| g:ViaService | Boolean | Whether the request is initiated by access forwarding from a cloud service on behalf of a principal. The value of this condition key is **true** only when **g:CalledVia** is not an empty string. This condition key is present only when a request is sent using STS Security Token. |
| g:VpcSourceIp | IP | Source IP address of a request initiated in a VPC. This condition key is present only when the request is initiated within a VPC and passes through a VPC endpoint to access a cloud service that is configured as a VPC endpoint service. |

1. **g:CalledVia**

   For example, a user makes a request to service A. Service A then makes a request to service B on behalf of the user, and service B makes a request to service C on behalf of the user. The request received by service A does not contain the g:CalledVia condition key because the requesting principal is a user. In the request received by service B, g:CalledVia contains the service principal of service A because the request is made by service A on behalf of the user. In the request received by service C, the g:CalledVia contains the service principals of service A and service B, and the sequence is the same as that of the forwarding access request chain. In this case, g:CalledViaFirst is the service principal of service A, and g:CalledViaLast is the service principal of service B. The g:CalledViaFirst and g:CalledViaLast condition keys can be used to specify the first and last services that are called in the forwarding access chain.

   **Figure 5-5** g:CalledVia application scenario



NOTE

When the user makes a request to a cloud service through the management console, CalledVia contains **service.console**.

For example, the following policy prevents the requests initiated on the management console from calling the RAM API for querying resource shares.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "ram:resourceShares:search"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "ForAnyValue:StringEquals": {
                "g:CalledVia": "service.console"
            }
        }
    }]
}
```

2. **g:CurrentTime**

   For example, the following policy prevents the invocation of cloud service APIs from March 1, 2023 to March 30, 2023.

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": ["ram:resourceShares:search"],
            "Resource": ["*"],
            "Condition": {
                "DateGreaterThan": {"g:CurrentTime": "2023-03-01T00:00:00Z"},
                "DateLessThan": {"g:CurrentTime": "2023-03-30T23:59:59Z"}
            }
        }
    ]
 }
```

3. **g:EnterpriseProjectId**

   This condition key is used in authentication. For example, the following policy prevents users from querying VPC permissions by enterprise project, and only denies access with **enterprise_project_id** set to **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx** in the request for calling the GET /v1/{project_id}/vpcs API.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "vpc:vpcs:list"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringEquals": {
                "g:EnterpriseProjectId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
            }
        }
    }]
}
```

   **NOTE**

   The g:EnterpriseProjectId condition key is not a filtering condition. This means resources in the enterprise project specified by this condition key will not be filtered out. In the example for calling the GET /v1/{project_id}/vpcs API, when **enterprise_project_id** is **all_granted_eps**, the VPCs associated with all enterprise projects of the user are queried. If this policy has been configured for the user, the VPCs associated with the enterprise project specified by **g:EnterpriseProjectId** in the policy will not be queried.

4. **g:MFAPresent**

This condition key is present only when a request is sent using STS Security Token. If a request is sent using permanent credentials, this condition key is not present.

For example, the following identity policy only allows API calling by principals authenticated using multi-factor authentication (MFA). The IfExists operator is used to cover scenarios where the g:MFAPresent condition key is not present when requests are made using permanent credentials.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "*"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "BoolIfExists": {
                "g:MFAPresent": "false"
            }
        }
    }]
}
```

5. **g:PrincipalUrn**

For example, the following SCP prevents the user **yyy** from creating resource shares.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "ram:resourceShares:create"
        ],
        "Condition": {
            "StringEquals": {
                "g:PrincipalUrn": "iam::xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx:user:yyy"
            }
        }
    }]
}
```

6. **g:PrincipalOrgId**

For example, the following policy prevents the accounts in organization **o-xxxxxxxxxxx** from calling the API for searching resource shares in RAM.

```
{
     "Version": "5.0",
     "Statement": [
         {
             "Effect": "Deny",
             "Action": ["ram:resourceShares:search"],
             "Resource": ["*"],
             "Condition": {
                 "StringEquals": {
                 "g:PrincipalOrgID": "o-xxxxxxxxxxx"

                 }
             }
         }
     ]
 }
```

7. **g:PrincipalOrgManagementAccountId**

For example, the condition key value **xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx** in the following identity policy matches the management account ID in the request.

```
{
    "Condition": {
        "StringEquals": {
            "g:PrincipalOrgManagementAccountId": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
        }
    }
}
```

8. **g:PrincipalOrgPath**

   For example, the condition key value **ou-qqq** in the following identity policy matches the organizational units (OUs) that the requesting principal belongs to in the request.

   ```
   {
       "Condition": {
           "StringMatch": {
               "g:PrincipalOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/*"
           }
       }
   }
   ```

   For example, the condition key value **ou-qqq** in the following identity policy matches any child OUs that the requesting principal belongs to in the request.

   ```
   {
       "Condition": {
           "StringMatch": {
               "g:PrincipalOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/ou-*"
           }
       }
   }
   ```

9. **g:PrincipalServiceName**

   For example, the condition key value **service.RAM** in the following policy matches the principal that is making the request.

   ```
   {
       "Condition": {
           "StringEquals": {
               "g:PrincipalServiceName": "service.RAM"
           }
       }
   }
   ```

10. **g:PrincipalTag/<tag-key>**

    For example, the following policy prevents IAM users tagged with {"department": "hr"} from accessing IAM APIs.

    ```
    {
        "Version": "5.0",
        "Statement": [{
            "Effect": "Deny",
            "Action": [
                "iam:*"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "g:PrincipalTag/department": "hr"
                }
            }
        }]
    }
    ```

11. **g:RequestTag/<tag-key>**

    For example, the following policy prevents users from creating resource shares tagged with {"team": "engineering"}.

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": ["ram:resourceShares:create"],
            "Resource": ["*"],
            "Condition": {
                "StringEquals": {
                    "g:RequestTag/team": "engineering"
                }
            }
        }
    ]
}
```

12. **g:ResourceAccount**

    For example, the following identity policy prevents users from using KMS keys of other than the specified users to decrypt data.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "g:ResourceAccount": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
            }
        }
    }]
}
```

13. **g:ResourceOrgId**

    For example, the following identity policy prevents users from using KMS keys of other than the specified organizations to decrypt data.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "g:ResourceOrgId": "o-xxxxxxxx"
            }
        }
    }]
}
```

14. **g:ResourceOrgPath**

    For example, the following policy prevents users from using KMS keys of the accounts in the **ou-qqq** OU to decrypt data.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringMatch": {
                "g:ResourceOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/*"
            }
        }
    }]
}
```

For example, the following policy prevents users from using KMS keys of the accounts in the child OUs under the **ou-qqq** OU to decrypt data.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringMatch": {
                "g:ResourceOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/ou-*"
            }
        }
    }]
}
```

15. **g:ResourceTag/<tag-key>**

    For example, the following policy prevents users from modifying resource shares tagged with {"team": "engineering"}.

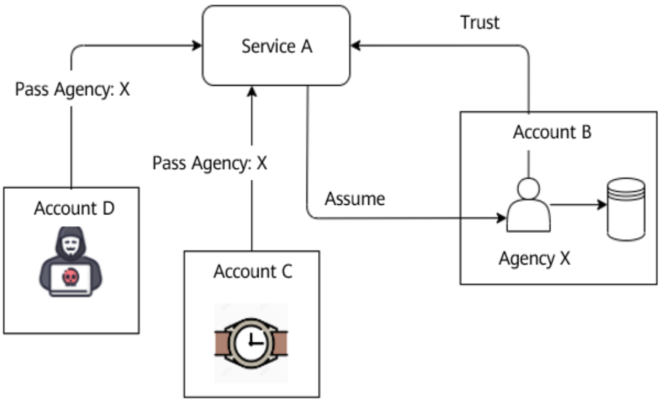
```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:delete",
        "ram:resourceShares:update"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "g:ResourceTag/team": "engineering"
        }
      }
    }
  ]
}
```

16. **g:SourceAccount**

    For example, service A is used to record activities. It helps a user (account B) to dump activity logs triggered by a device (account C) to a specified OBS bucket. To enable service A to write data into the bucket, the administrator of account B creates an agency or trust agency named X for service A to manage

OBS buckets under account B. After account B or account C accesses service A and triggers a request, service A obtains the temporary identity credentials of the specified agency or trust agency X and writes data to the bucket.

**Figure 5-6** Confused deputy



The agency or trust agency name X is not confidential. If an attacker (account D) obtains the agency name and triggers service A in the same way, the activity records of the attacker would be incorrectly recorded in the OBS bucket. The attacker uses service A's agency to indirectly modify the OBS bucket of account B. This is called the confused deputy.

The g:SourceAccount condition key is used to control the account of the resource making a service-to-service request. The following policy only allows service A to switch to the assumed-agency session for account **xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx** or **yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy**.

```
{
    "Version": "5.0",
    "Statement": [{
        "Principal": {
            "Service": [
                "Service.A"
            ]
        },
        "Action": [
            "sts:agencies:assume"
        ],
        "Condition": {
            "StringEquals": {
                "g:sourceAccount": [
                    "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
                    "yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy"
                ]
            }
        }
    }]
}
```

17. **g:SourceUrn**

Similar to g:SourceAccount, this condition key is also used to solve the confused deputy issue. Assume that user devices (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx) are defined as watches and bracelets. The g:SourceUrn condition key is used to control the URN of the resource making a service-to-service request. The following policy only allows service A to switch to the corresponding assumed-agency session for the watch or bracelet that meets the conditions.

```
{
    "Version": "5.0",
    "Statement": [{
        "Principal": {
            "Service": [
                "Service.A"
            ]
        },
        "Action": [
            "sts:agencies:assume"
        ],
        "Condition": {
            "StringEquals": {
                "g:sourceUrn": [
                    "alarm:*:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx:watch:*",
                    "alarm:*:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx:bracelet:*"
                ]
            }
        }
    }]
}
```

18. **g:SourceIdentity**

    For example, the following policy prevents principals whose **source_identity** is **yyyyy** from switching the agency.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Principal": {
            "IAM": [
                "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
            ]
        },
        "Action": [
            "sts:agencies:assume"
        ],
        "Condition": {
            "StringEquals": {
                "g:SourceIdentity": "yyyyy"
            }
        }
    }]
}
```

19. **g:SourceIp**

    For example, the following policy denies the programmatic or console access to KMS from source IP addresses within the xxx.xx.xx.0/24 range.

NOTICE

The source IP address must be a public IP address. Do not include a private IP address in the condition key.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "IpAddress": {
                "g:SourceIp": "xxx.xx.xx.0/24"
            }
        }
    }]
}
```

The following condition keys in the initial request context will not be passed in subsequent requests forwarded by the service on behalf of the principal: g:SourceIp, g:SourceVpce, g:SourceVpc, and g:VpcSourceIp. As a result, when these condition keys are used to control access permissions, requests forwarded by the cloud service on behalf of the principal may be denied. In practice, you are advised to use g:CalledVia to forward access requests.

There is an exception: The public network access initiated by the principal from the console can be regarded as a programmatic access of the principal from the public network, so the request forwarded by the console on behalf of the principal contains the initial g:SourceIp.

For example, the following policy denies the programmatic or console access to KMS from source IP addresses beyond xxx.xx.xx.0/24. In addition, the policy allows cloud services to forward access requests on behalf of the principal.

```
{
    "Version": "5.0",
    "Statement": [{
            "Effect": "Deny",
            "Action": [
                "kms:cmk:decryptData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "NotIpAddress": {
                    "g:SourceIp": "xxx.xx.xx.0/24"
                },
                "Bool": {
                    "g:ViaService": "false"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "kms:cmk:decryptData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "NotIpAddress": {
                    "g:SourceIp": "xxx.xx.xx.0/24"
                },
                "StringEqualsIfExists": {
                    "g:CalledViaFirst": "service.console",
                    "g:CalledViaLast": "service.console"
                }
            }
        }
    ]
}
```

20. **g:SourceVpce**

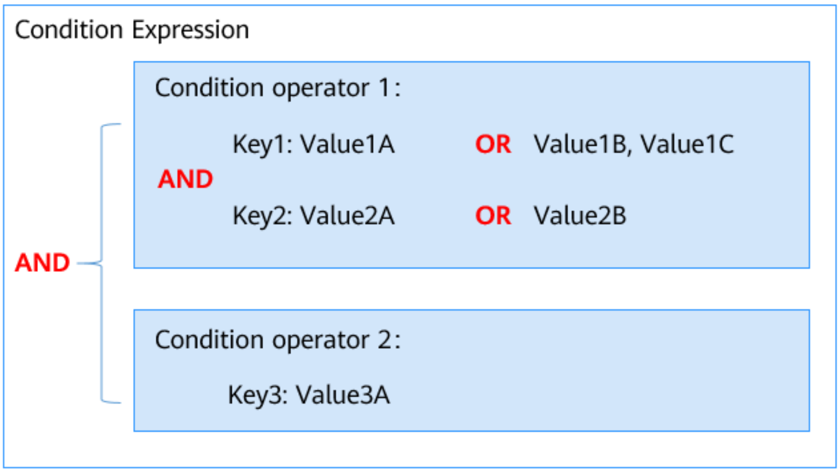
    For example, the following policy denies access to KMS from a VPC endpoint other than **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**. In addition, the policy allows cloud services to forward access requests on behalf of the principal.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "g:SourceVpce": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
            },
            "Bool": {
                "g:ViaService": "false"
            }
        }
    }]
}
```

- Multivalued condition keys
  a. ForAllValues: Tests whether the value of every member of the request set is a subset of the condition key set. The condition returns true if every key value in the request matches at least one value in the policy.
  b. ForAnyValue: Tests whether at least one member of the set of request values matches at least one member of the set of condition key values. The condition returns true if any one of the key values in the request matches any one of the condition values in the policy. The condition returns false if there are no matching keys in the request, or if the key value resolves to an empty data set.

     **Condition Operators**

     **Figure 5-7** Condition operators



     i. If a single condition operator includes multiple values for one key, that condition operator is evaluated using a logical OR. The condition returns **true** if any one of the key values in the request matches any one of the condition values in the policy.

NOTICE

For condition operators that contain Not (such as StringNotEquals), the request value cannot match any of the condition values.

ii. The AND operation is used between different condition keys of the same operator. It is also used between different operators.

## Operators

A condition operator, a condition key, and a condition value together constitute a complete condition statement. A policy can be applied only when its request conditions are met. The operator suffix **IfExists** indicates that a policy is applied if a request value is empty or meets the specified condition. For example, if the operator **StringEqualsIfExists** is selected for a policy, the policy is applied if a request value is empty or equal to the specified condition value. Operators are string operators. They are not case-sensitive unless otherwise specified.

- String

**Table 5-3** String condition operators

| Type | Operator | Description |
|---|---|---|
| String | StringEquals | Exact matching, case sensitive |
| | StringNotEquals | Negated matching, case sensitive |
| | StringEqualsIgnoreCase | Exact matching, ignoring case |
| | StringNotEqualsIgnoreCase | Negated matching, ignoring case |
| | StringMatch | Case-sensitive matching. The values can include multi-character match wildcards (*) and single-character match wildcards (?) anywhere in the string. |
| | StringNotMatch | Negated case-sensitive matching. The values can include multi-character match wildcards (*) and single-character match wildcards (?) anywhere in the string. |

For example, the following policy prevents the requester Tom from deleting or modifying resource shares.

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:resourceShares:delete",
                "ram:resourceShares:update"
            ],
            "Condition": {
                "StringEquals": {
                    "g:DomainName": [
                        "Tom"
                    ]
                }
            }
        }
    ]
}
```

- Numeric

**Table 5-4** Numeric condition operators

| Type | Operator | Description |
|---|---|---|
| Numeric | NumberEquals | Matching |
| | NumberNotEquals | Negated matching |
| | NumberLessThan | "Less than" matching |
| | NumberLessThanEquals | "Less than or equals" matching |
| | NumberGreaterThan | "Greater than" matching |
| | NumberGreaterThanEquals | "Greater than or equals" matching |

- Date

**Table 5-5** Date condition operators

| Type | Operator | Description |
|---|---|---|
| Date | DateLessThan | Matching before a specific date and time |
| | DateLessThanEquals | Matching at or before a specific date and time |
| | DateGreaterThan | Matching after a specific date and time |
| | DateGreaterThanEquals | Matching at or after a specific date and time |

For example, the following policy prevents requesters from accessing RAM before August 1, 2022.

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:*:*"
            ],
            "Condition": {
                "DateLessThan": {
                    "g:CurrentTime": [
                        "2022-08-01T00:00:00Z"
                    ]
                }
            }
        }
    ]
}
```

- Boolean

**Table 5-6** Boolean condition operators

| Type | Operator | Description |
|---|---|---|
| Bool | Bool | Boolean conditions let you construct condition elements that restrict access based on comparing a key to "true" or "false." |

- Null

**Table 5-7** Null condition operators

| Type | Operator | Description |
|---|---|---|
| Null | Null | You can use a Null condition operator to check if a condition key is absent at the time of authorization. In the policy statement, you can use either "true" (the key does not exist or is null) or "false" (the key exists and its value is not null). |

- IP

**Table 5-8** IP condition operators

| Type | Operator | Description |
|---|---|---|
| IP | IpAddress | IP address or IP address range |
| | NotIpAddress | All IP addresses beyond a specific IP address or IP address range |

For example, the following policy prevents requests from the IP address range (10.27.128.0 to 10.27.128.255) from modifying the specified permanent access keys.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "iam:credentials:updateCredentialV5"
      ],
      "Condition": {
        "IpAddress": {
          "g:SourceIp": [
            "10.27.128.0/24"
          ]
        }
      }
    }
  ]
}
```

- IfExists operator suffix

  You can add "IfExists" to the end of any condition operator name except the "Null condition", for example, StringEqualsIfExists. If the policy key is present in the context of the request, process the key as specified in the policy. If the key is not present, evaluate the condition element as true.

# 5.2 Enabling or Disabling the SCP Type

## Enabling the SCP Type

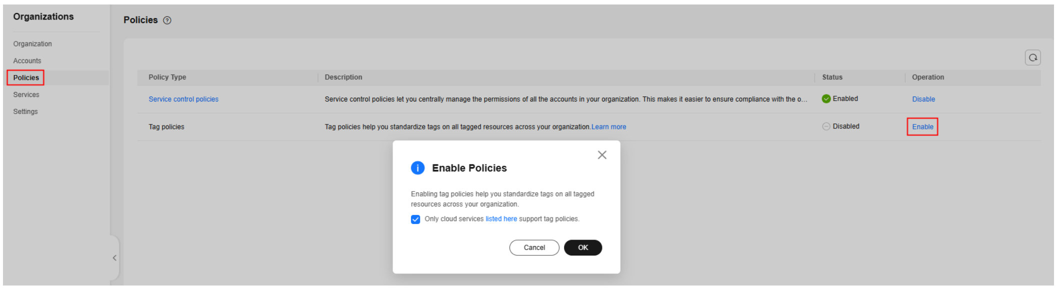
Before you create and attach an SCP to OUs and accounts, you have to enable the SCP type from the organization's management account. After the SCP type is enabled, Organizations automatically attach the FullAccess policy (allowing for all operations) to all OUs and accounts.

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Policies** page, click **Enable** in the **Operation** column of the service control policies.

**Step 3** In the displayed dialog box, select the check box and click **OK**.

**Figure 5-8** Enabling the SCP type



| Policy Type | Description | Status | Operation |
|---|---|---|---|
| Service control policies | Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it easier to ensure compliance with the o... | Enabled | Disable |
| Tag policies | Tag policies help you standardize tags on all tagged resources across your organization. Learn more | Disabled | Enable |

Enable Policies

Enabling tag policies help you standardize tags on all tagged resources across your organization.

☑ Only cloud services listed here support tag policies.

Cancel OK

**----End**

## Disabling the SCP type

If you no longer want to use SCPs to manage permissions for your organization, you can disable the SCP type from the organization's management account.

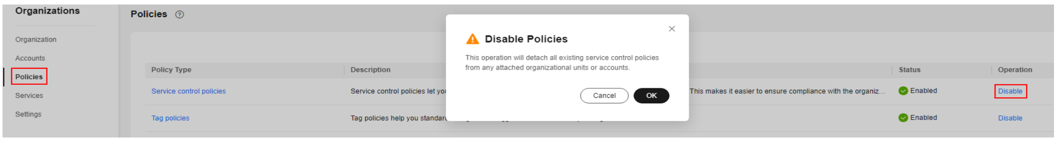
⚠ CAUTION

- After the SCP type is disabled in an organization, all SCPs are automatically detached from all OUs and accounts in the organization. However, the SCPs are not deleted.
- If you disable the SCP type and then enable it again, the FullAccess SCP is still attached to all entities in the organization and attachments of other SCPs are lost. If you want to re-enable them, you must re-attach them to the entities.

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Policies** page, click **Disable** in the **Operation** column of the service control policies.

**Figure 5-9** Disabling the SCP type



Disable Policies

This operation will detach all existing service control policies from any attached organizational units or accounts.

| Policy Type | Description | Status | Operation |
|---|---|---|---|
| Service control policies | Service control policies let yo... This makes it easier to ensure compliance with the organiz... | Enabled | Disable |
| Tag policies | Tag policies help you standar... | Enabled | Disable |

**Step 3** Click **OK** in the displayed dialog box.

**----End**

# 5.3 Creating an SCP

This topic describes how to create a custom SCP. For SCP examples, see **Example SCPs**.

## Constraints

- Effect in a custom SCP can only be set to Deny.
- Only Action is supported. NotAction is not supported.
- The action prefix must be the name of a cloud service that has been interconnected with IAM 5.0, for example, Action="ram:*:*". Wildcards (*) are not supported for prefixes. For example, Action="*" or Action="*:*:*" is not allowed.
- An action in a custom SCP must contain three fields and have the following structure:

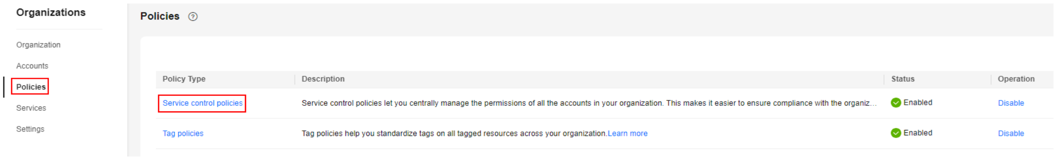
  "service-name:type-name:action-name"

## Procedure

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Policies** page, click **Service control policies**.

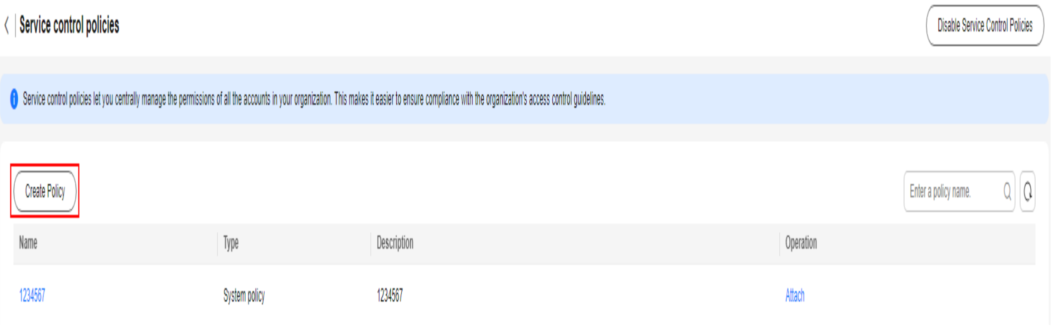
**Figure 5-10** Accessing the **Service control policies** page



| Policy Type | Description | Status | Operation |
|---|---|---|---|
| Service control policies | Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it easier to ensure compliance with the organiz... | ✓ Enabled | Disable |
| Tag policies | Tag policies help you standardize tags on all tagged resources across your organization.Learn more | ✓ Enabled | Disable |

**Step 3** Click **Create Policy**.

**Figure 5-11** Creating an SCP

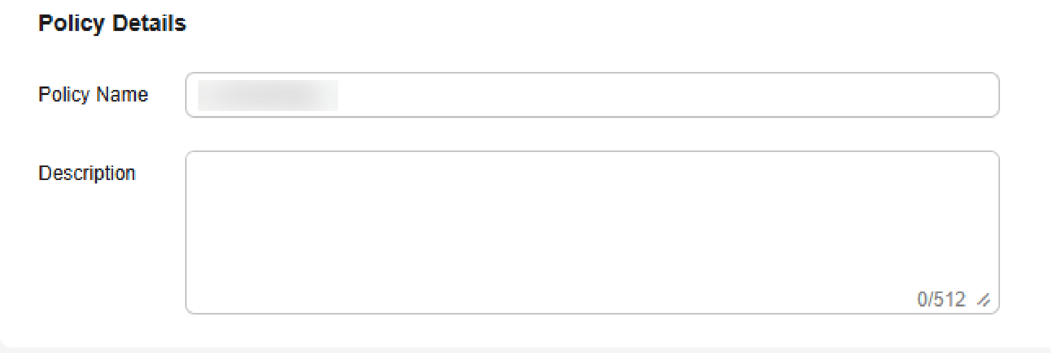


Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it easier to ensure compliance with the organization's access control guidelines.

| Name | Type | Description | Operation |
|---|---|---|---|
| 1234567 | System policy | 1234567 | Attach |

**Step 4** Enter a policy name. Ensure that you are entering a unique policy name. It must be different from any other existing policy.

(Optional) You can also enter a description for the policy.



Policy Details

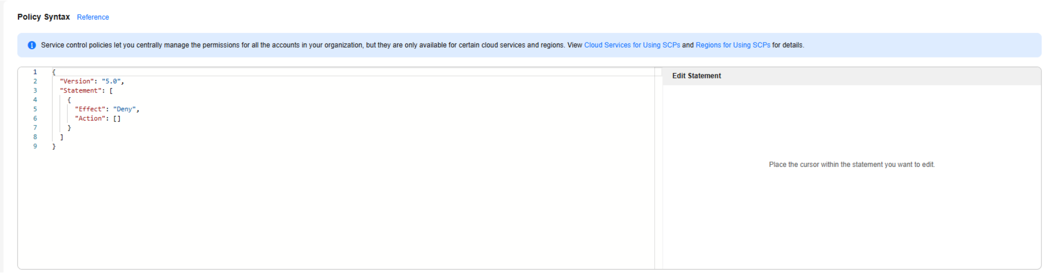
Policy Name

Description

0/512

**Step 5** On the left of the policy content, edit the policy content in JSON.

For details about how to build JSON policy statements, see **SCP Syntax** and **Example SCPs**.



Policy Syntax Reference

Service control policies let you centrally manage the permissions for all the accounts in your organization, but they are only available for certain cloud services and regions. View Cloud Services for Using SCPs and Regions for Using SCPs for details.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": []
    }
  ]
}
```

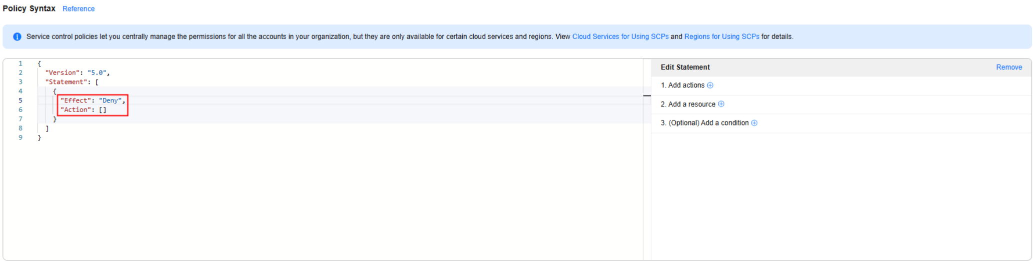
Edit Statement

Place the cursor within the statement you want to edit.

NOTE

The **Version** value of a custom policy must be **5.0**.

**Step 6** Hover over the statement on the left of the policy content, and edit the actions, resources, and conditions of the custom policy in the policy editor on the right.



Policy Syntax Reference

Service control policies let you centrally manage the permissions for all the accounts in your organization, but they are only available for certain cloud services and regions. View Cloud Services for Using SCPs and Regions for Using SCPs for details.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": []
    }
  ]
}
```

Edit Statement Remove

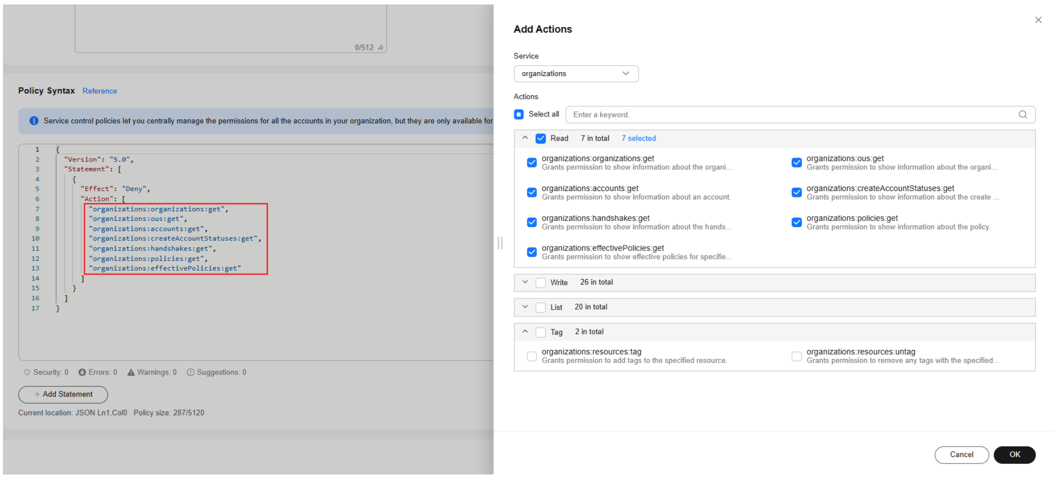
1. Add actions ⊕

2. Add a resource ⊕

3. (Optional) Add a condition ⊕

- Adding an action: You can click ⊕, and select or search for the service and action to be added. The added action will be displayed in **Action** on the left of the policy content. **Figure 5-12** shows the details.

**Figure 5-12** Adding an action



0/512

Policy Syntax Reference

Service control policies let you centrally manage the permissions for all the accounts in your organization, but they are only available for

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "organizations:organizations:get",
        "organizations:ous:get",
        "organizations:accounts:get",
        "organizations:createAccountStatuses:get",
        "organizations:handshakes:get",
        "organizations:policies:get",
        "organizations:effectivePolicies:get"
      ]
    }
  ]
}
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

+ Add Statement

Current location: JSON Ln1,Col0 Policy size: 287/5120

Add Actions

Service: organizations

Actions

■ Select all Enter a keyword.

☑ Read 7 in total 7 selected

☑ organizations:organizations:get
Grants permission to show information about the organi...

☑ organizations:ous:get
Grants permission to show information about the organi...

☑ organizations:accounts:get
Grants permission to show information about an account.

☑ organizations:createAccountStatuses:get
Grants permission to show information about the create ...

☑ organizations:handshakes:get
Grants permission to show information about the hands...

☑ organizations:policies:get
Grants permission to show information about the policy.

☑ organizations:effectivePolicies:get
Grants permission to show effective policies for specifie...

□ Write 26 in total

□ List 20 in total

□ Tag 2 in total

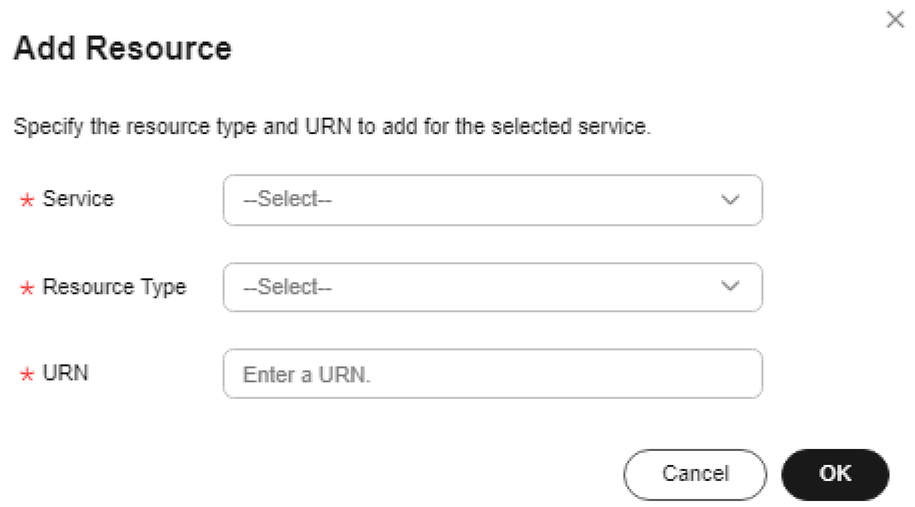
□ organizations:resources:tag
Grants permission to add tags to the specified resource.

□ organizations:resources:untag
Grants permission to remove any tags with the specified...

Cancel OK

- Adding a resource: Only services available for resource-level authorization can be added. You can click ⊕ to select a service and resource type and enter the URN as required, as shown in **Figure 5-13**.

**Figure 5-13** Adding a resource



Add Resource

Specify the resource type and URN to add for the selected service.

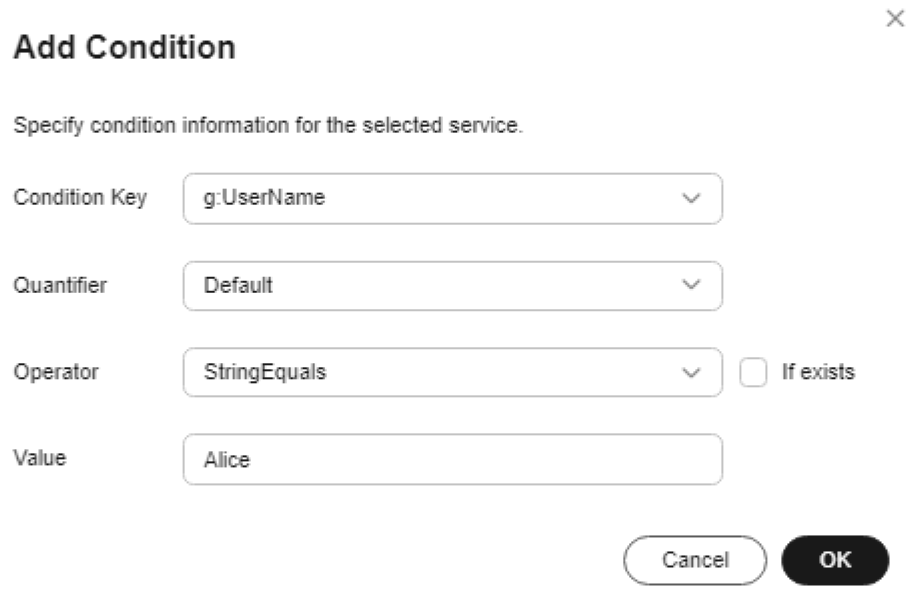
* Service: --Select--

* Resource Type: --Select--

* URN: Enter a URN.

- (Optional) Adding a condition: You can click ⊕ to add a condition key and a condition operator to define the conditions for the policy to take effect, as shown in **Figure 5-14**.

**Figure 5-14** Adding a condition



Add Condition

Specify condition information for the selected service.

Condition Key: g:UserName

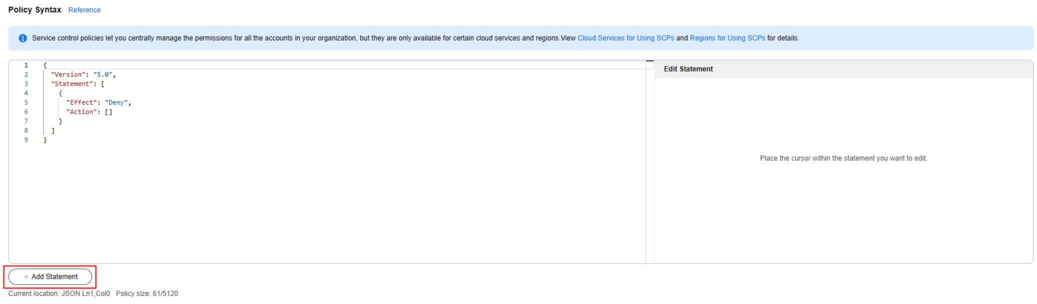
Quantifier: Default

Operator: StringEquals □ If exists

Value: Alice

**Step 7** (Optional) Click **Add Statement** to add an object for the Statement element.

The value for the Statement element can be an array of multiple objects that identify different permissions.



Policy Syntax Reference

Service control policies let you centrally manage the permissions for all the accounts in your organization, but they are only available for certain cloud services and regions. View Cloud Services for Using SCPs and Regions for Using SCPs for details.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": []
    }
  ]
}
```

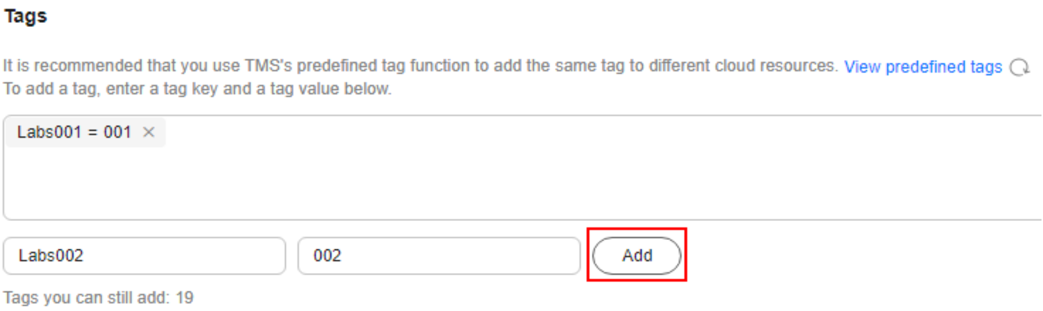
Edit Statement

Place the cursor within the statement you want to edit.

Current location: JSON Ln1,Col0 Policy size: 61/5120

**Step 8** (Optional) Add one or more tags. Enter a tag key and a tag value, and click **Add**.

**Figure 5-15** Adding tags to the SCP



Tags

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

To add a tag, enter a tag key and a tag value below.

Labs001 = 001

Labs002

002

Tags you can still add: 19

**Step 9** Click **Save**. If the policy list is displayed, the SCP is created successfully. If a message appears indicating incorrect policy content, modify the SCP syntax.

**----End**

# 5.4 Modifying or Deleting an SCP

The following describes how to modify and delete a custom SCP.

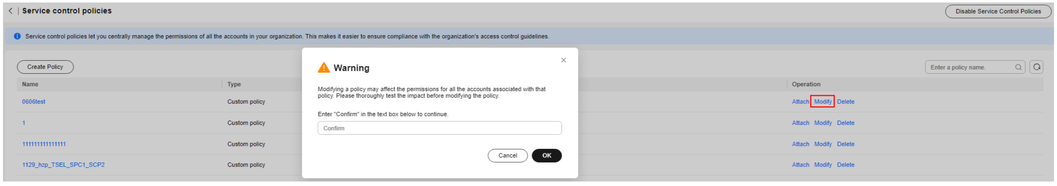
## Modifying an SCP

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Policies** page, click **Service control policies**.

**Step 3** Locate the custom SCP you want to modify and click **Edit** in the **Operation** column. In the displayed dialog box, enter "Confirm" and click **OK**.

**Figure 5-16** Modifying an SCP



Service control policies

Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it easier to ensure compliance with the organization's access control guidelines.

| Name | Type | Operation |
|---|---|---|
| 0606test | Custom policy | Attach Modify Delete |
| 1 | Custom policy | Attach Modify Delete |
| 111111111111111 | Custom policy | Attach Modify Delete |
| 1129_hzp_TSEL_SPC1_SCP2 | Custom policy | Attach Modify Delete |

Warning

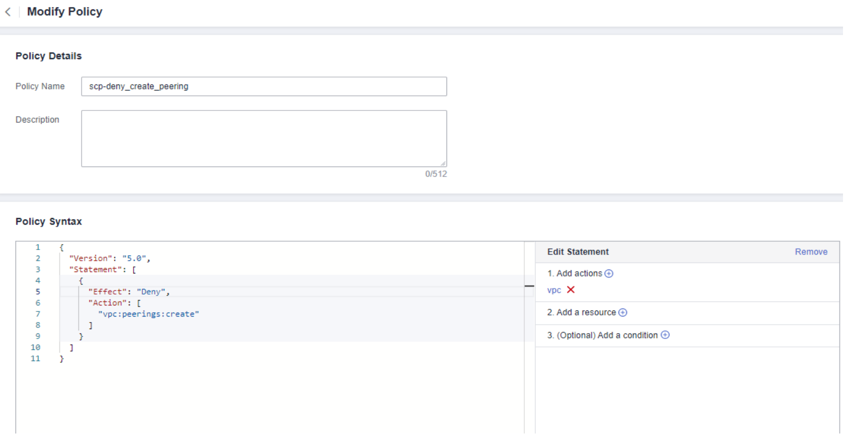
Modifying a policy may affect the permissions for all the accounts associated with that policy. Please thoroughly test the impact before modifying the policy.

Enter "Confirm" in the text box below to continue.

Confirm

**Step 4** On the **Modify Policy** page, modify the policy name and description as needed, as shown in**Figure 5-17**.

**Figure 5-17** Modifying an SCP



Modify Policy

Policy Details

Policy Name: scp-deny_create_peering

Description:

0/512

Policy Syntax

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "vpc:peerings:create"
      ]
    }
  ]
}
```

Edit Statement

Remove

1. Add actions

vpc

2. Add a resource

3. (Optional) Add a condition

**Step 5** Edit the policy content if needed. You can use the statement editor to modify the policy syntax. For details, see **SCP Syntax**.

**Step 6** Click **Save**. If the policy list is displayed, the SCP is updated successfully. If a message appears indicating incorrect policy content, modify the SCP syntax.

**----End**

## Deleting an SCP

An SCP that is attached to OUs or accounts cannot be deleted. To delete such an SCP, you need to detach the SCP from the OUs or accounts first.

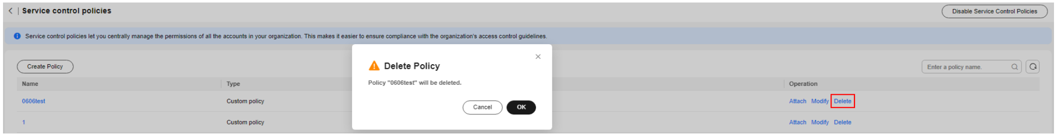
**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Policies** page, click **Service control policies**.

**Step 3** Locate the target custom SCP and click **Delete** in the **Operation** column.

**Step 4** Click **OK** in the displayed dialog box.

**Figure 5-18** Deleting an SCP



Service control policies

Disable Service Control Policies

Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it easier to ensure compliance with the organization's access control guidelines.

Create Policy

Enter a policy name.

| Name | Type | Operation |
|---|---|---|
| 0606test | Custom policy | Attach Modify Delete |
| 1 | Custom policy | Attach Modify Delete |

Delete Policy

Policy "0606test" will be deleted.

Cancel OK

**----End**

# 5.5 Attaching or Detaching an SCP

You can attach an SCP to or detach it from the root OU, other OUs or accounts from the organization's management account.

## Constraints

- SCPs affect only member accounts in an organization. They have no effect on the management account, IAM users, and agencies.

- SCPs are applied within 30 minutes after they are attached.

## Attaching an SCP

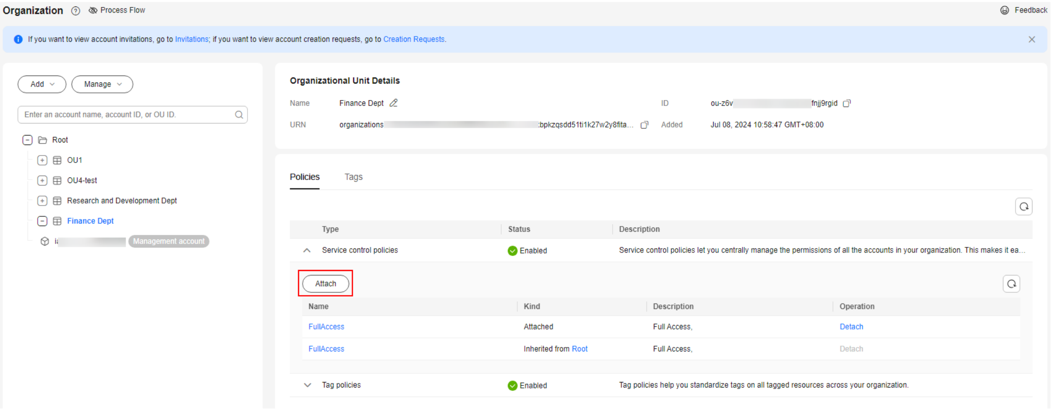
**Method 1:**

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the OU or account you want to attach the SCP to.

**Step 3** On the details page, click the **Policies** tab. On the page, expand **Service control policies** and click **Attach**.

**Figure 5-19** Attaching an SCP



If you want to view account invitations, go to Invitations; if you want to view account creation requests, go to Creation Requests.

Organizational Unit Details

Name: Finance Dept

ID: ou-z6v[redacted]fnjj9rgid

URN: organizations[redacted]:bpkzqsdd51ti1k27w2y8fita...

Added: Jul 08, 2024 10:58:47 GMT+08:00

| Type | Status | Description |
|---|---|---|
| Service control policies | Enabled | Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it ea... |
| Tag policies | Enabled | Tag policies help you standardize tags on all tagged resources across your organization. |

| Name | Kind | Description | Operation |
|---|---|---|---|
| FullAccess | Attached | Full Access, | Detach |
| FullAccess | Inherited from Root | Full Access, | Detach |

**Step 4** Select the policy to be added and enter "Confirm" in the text box. Then, click **Attach**.

**----End**

**Method 2:**

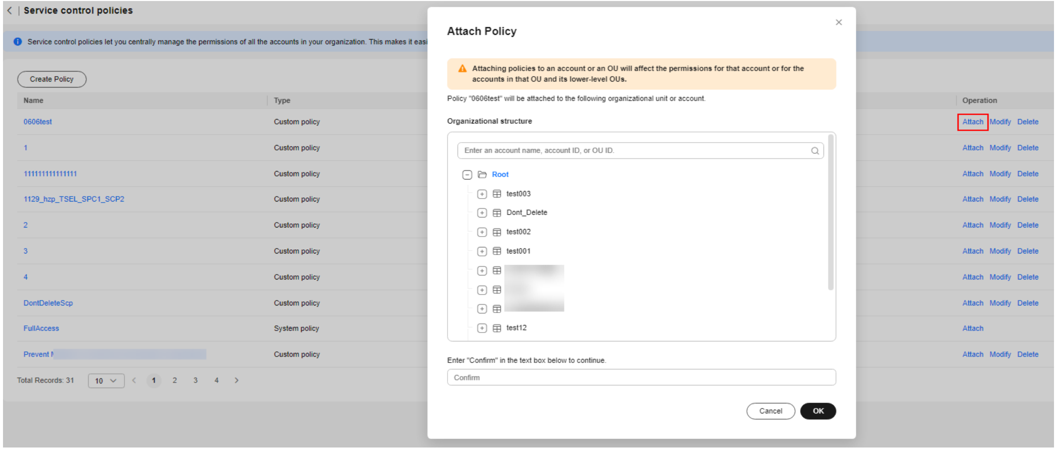
**Step 1** Access the **Policies** page on the Organizations console.

**Step 2** Click **Service control policies**. The list of SCPs is displayed.

**Step 3** Locate the SCP you want to attach and click **Attach** in the **Operation** column. Then, select the OU or account you want to attach the SCP to.

**Step 4** In the displayed dialog box, enter "Confirm" and click **OK**.In the displayed dialog box, click **OK**.

**Figure 5-20** Attaching an SCP



Service control policies

Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it easi

| Name | Type | Operation |
|---|---|---|
| 0606test | Custom policy | Attach Modify Delete |
| 1 | Custom policy | Attach Modify Delete |
| 11111111111111 | Custom policy | Attach Modify Delete |
| 1129_hzp_TSEL_SPC1_SCP2 | Custom policy | Attach Modify Delete |
| 2 | Custom policy | Attach Modify Delete |
| 3 | Custom policy | Attach Modify Delete |
| 4 | Custom policy | Attach Modify Delete |
| DontDeleteScp | Custom policy | Attach Modify Delete |
| FullAccess | System policy | Attach |
| Prevent [redacted] | Custom policy | Attach Modify Delete |

Total Records: 31 10 1 2 3 4

Attach Policy

Attaching policies to an account or an OU will affect the permissions for that account or for the accounts in that OU and its lower-level OUs.

Policy "0606test" will be attached to the following organizational unit or account.

Organizational structure

Enter an account name, account ID, or OU ID.

- Root
  - test003
  - Dont_Delete
  - test002
  - test001
  - [redacted]
  - test12

Enter "Confirm" in the text box below to continue.

Confirm

**----End**

## Detaching an SCP

**Method 1**:

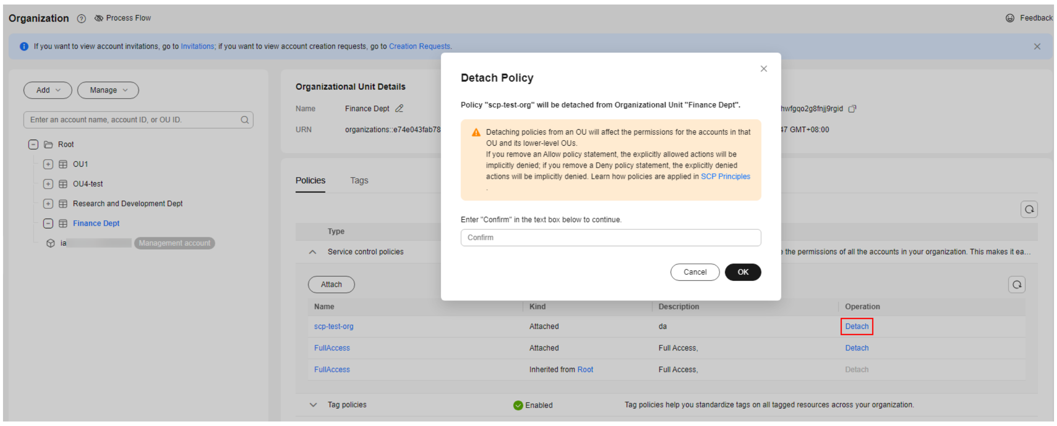
**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the OU or account you want to detach the SCP from.

**Step 3** On the details page, click the **Policies** tab. On the page, expand **Service control policies**, locate the target SCP and click **Detach** in the **Operation** column.

**Step 4** In the displayed dialog box, enter "Confirm" and click **OK**.In the displayed dialog box, click **OK**.

**Figure 5-21** Detaching an SCP



If you want to view account invitations, go to Invitations; if you want to view account creation requests, go to Creation Requests.

Enter an account name, account ID, or OU ID.

- Root
  - OU1
  - OU4-test
  - Research and Development Dept
  - Finance Dept
    - ia[redacted] Management account

Organizational Unit Details

Name Finance Dept

URN organizations::e74e043fab78

hwfgqo2g8fnjj9rgid

47 GMT+08:00

Type

Service control policies

the permissions of all the accounts in your organization. This makes it ea...

| Name | Kind | Description | Operation |
|---|---|---|---|
| scp-test-org | Attached | da | Detach |
| FullAccess | Attached | Full Access, | Detach |
| FullAccess | Inherited from Root | Full Access, | Detach |

Tag policies Enabled Tag policies help you standardize tags on all tagged resources across your organization.

Detach Policy

Policy "scp-test-org" will be detached from Organizational Unit "Finance Dept".

Detaching policies from an OU will affect the permissions for the accounts in that OU and its lower-level OUs.
If you remove an Allow policy statement, the explicitly allowed actions will be implicitly denied; if you remove a Deny policy statement, the explicitly denied actions will be implicitly denied. Learn how policies are applied in SCP Principles
.

Enter "Confirm" in the text box below to continue.

Confirm

NOTE

You cannot detach the last SCP from an OU or account. There must be at least one SCP attached to every OU or account.

**----End**

**Method 2:**

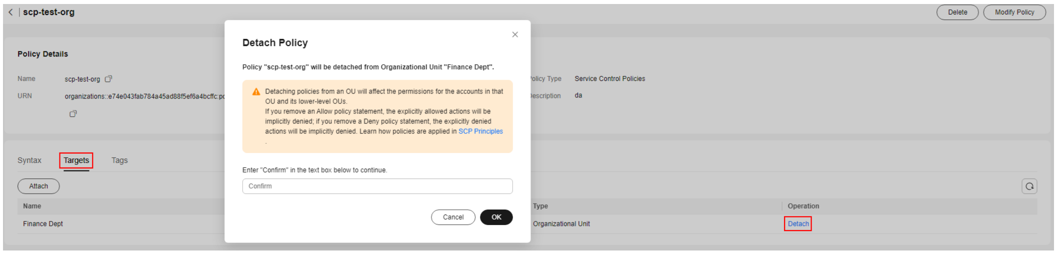
**Step 1** Access the **Policies** page on the Organizations console.

**Step 2** Click **Service control policies**. The list of SCPs is displayed.

**Step 3** Click the name of the target SCP and click the **Targets** tab.

**Step 4** Locate the OU or account from which the SCP is to be detached and click **Detach** in the **Operation** column. In the displayed dialog box, enter "Confirm" and click **OK**.

**Figure 5-22** Detaching an SCP



scp-test-org

Policy Details

Name scp-test-org

URN organizations::e74e043fab784a45ad88f5ef6a4bcffc:pc

olicy Type Service Control Policies

escription da

Detach Policy

Policy "scp-test-org" will be detached from Organizational Unit "Finance Dept".

Detaching policies from an OU will affect the permissions for the accounts in that OU and its lower-level OUs.
If you remove an Allow policy statement, the explicitly allowed actions will be implicitly denied; if you remove a Deny policy statement, the explicitly denied actions will be implicitly denied. Learn how policies are applied in SCP Principles
.

Enter "Confirm" in the text box below to continue.

Confirm

| Name | Type | Operation |
|---|---|---|
| Finance Dept | Organizational Unit | Detach |

**----End**

# 5.6 Example SCPs

This section provides some example SCPs for your reference, including:

- Preventing Member Accounts from Leaving an Organization
- Blocking Service Access for the Root User
- Prohibiting Creation of Resources with Specified Tags
- Prohibiting Access to Specified Regions
- Preventing Sharing with Accounts Outside an Organization
- Preventing Sharing Specified Resource Types
- Preventing Aggregation Authorization to Accounts Outside the Current Organization
- Preventing IAM Users and Agencies from Making Certain Changes
- Preventing IAM Users and Agencies from Making Specified Changes, with an Exception for Specified Accounts
- Preventing IAM Users and Agencies from Making Specified Changes, with an Exception for Specified Agencies

## Preventing Member Accounts from Leaving an Organization

The following SCP prevents member accounts from leaving an organization.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "organizations:organizations:leave"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

## Blocking Service Access for the Root User

The following SCP blocks access to the specified actions for the root user in a member account. If you want to restrict access in specific ways, you can modify the Action and Resource elements.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ecs:*:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "BoolIfExists": {
          "g:PrincipalIsRootUser": "true"
        }
      }
    }
  ]
}
```

## Prohibiting Creation of Resources with Specified Tags

The following SCP prevents users from creating resource shares with the {"team": "engineering"} tag. If you want to prevent resource creation in specific ways, you can modify the Action, Resource, and Condition elements.

```
{
    "Version":"5.0",
    "Statement":[
        {
            "Effect":"Deny",
            "Action":["ram:resourceShares:create"],
            "Resource":["*"],
            "Condition":{
                "StringEquals":{
                    "g:RequestTag/team":"engineering"
                }
            }
        }
    ]
 }
```

## Prohibiting Access to Specified Regions

The following SCP prevents users from accessing all ECS resources in **regionid1** but not in any other regions. If you want to restrict access in specific ways, you can modify the Action, Resource, and Condition elements.

This SCP applies only to region-specific services. **regionid1** in the SCP is only an example for you reference. Enter the specific region ID you want when using this SCP.

```
{
    "Version":"5.0",
    "Statement":[
        {
            "Effect":"Deny",
            "Action":["ecs:*:*"],
            "Resource":["*"],
            "Condition":{
                "StringEquals":{
                    "g:RequestedRegion":"ap-southeast-1"
                }
            }
        }
    ]
 }
```

## Preventing Sharing with Accounts Outside an Organization

The following SCP prevents accounts within an organization from sharing resources with accounts outside the organization. You are advised to attach this SCP to the root OU of the organization so that the SCP will be applied to the entire organization.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:create",
        "ram:resourceShares:associate"

      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAnyValue:StringNotLike": {
          "ram:TargetOrgPaths": [
            "organization_id/root_id/ou_id" [Note: Enter the path ID of the organization.]
          ]
        }
      }
    }
  ]
}
```

## Preventing Sharing Specified Resource Types

The following SCP prevents accounts from sharing VPC subnets. You can modify the resource type in the Condition element of the SCP statement as required.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "ram:RequestedResourceType": [
      "vpc:subnet" [Note: You can change the resource type as required.]
     ]
    }
   }
  }
 ]
}
```

## Preventing Aggregation Authorization to Accounts Outside the Current Organization

The following SCP prevents accounts within an organization from granting aggregation authorization to accounts outside the organization. You are advised to attach this SCP to the root OU of your organization to prevent accounts outside your organization from collecting information about the resources of accounts in your organization. You can also attach this SCP to source accounts to prevent them from accepting authorization requests from the aggregator account.

```
{
 "Version": "5.0",
 "Statement": [
  {
   "Effect": "Deny",
   "Action": [
    "rms:aggregationAuthorizations:create"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringNotMatch": {
     "rms:AuthorizedAccountOrgPath": [
      "organization_id/root_id/ou_id" [Note: Enter the path ID of the organization.]
     ]
    }
   }
  }
 ]
}
```

## Preventing IAM Users and Agencies from Making Certain Changes

The following SCP prevents IAM users and agencies from making changes to resource shares created in all accounts in your organization.

```
{
 "Version": "5.0",
 "Statement": [
  {
   "Effect": "Deny",
   "Action": [
    "ram:resourceShares:update",
    "ram:resourceShares:delete",
    "ram:resourceShares:associate",
    "ram:resourceShares:disassociate",
    "ram:resourceShares:associatePermission",
    "ram:resourceShares:disassociatePermission"
   ],
   "Resource": [
    "ram::*:resourceShare:resource-id"
   ]
  }
 ]
}
```

### Preventing IAM Users and Agencies from Making Specified Changes, with an Exception for Specified Accounts

The following SCP prevents IAM users and agencies from making changes to resource shares created in all accounts in your organization except for specified accounts.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:update",
        "ram:resourceShares:delete",
        "ram:resourceShares:associate",
        "ram:resourceShares:disassociate",
        "ram:resourceShares:associatePermission",
        "ram:resourceShares:disassociatePermission"
      ],
      "Resource": [
        "ram::*:resourceShare:resource-id"
      ],
      "Condition": {
        "StringNotEquals": {
          "g:DomainId": [
            "account-id" [Note: Enter the ID of the account to deny.]
          ]
        }
      }
    }
  ]
}
```

### Preventing IAM Users and Agencies from Making Specified Changes, with an Exception for Specified Agencies

The following SCP prevents IAM users and agencies from making changes to resource shares created in all accounts in your organization except for specified agencies.

```
{
   "Version": "5.0",
   "Statement": [
     {
       "Effect": "Deny",
       "Action": [
         "ram:resourceShares:create"
       ],
       "Resource": [
         "*"
       ],
       "Condition": {
         "StringNotMatch": {
           "g:PrincipalUrn": "sts::*:assumed-agency:AgencyName/*"
         }
       }
     }
   ]
 }
```

## 5.7 System-defined SCPs

The following table lists the SCPs preconfigured on Huawei Cloud.

**Table 5-9** Huawei Cloud SCPs

| Policy | Description |
|---|---|
| FullAccess | Allows all permissions on all resources. |

NOTE

At least one SCP must be attached to each root, OU, and account.

# 5.8 Cloud Services for Using SCPs

SCPs are available for the following cloud services:

NOTE

Cloud services for using SCPs also support IAM identity policies.

## Management & Deployment

| No. | Service Name | Reference |
|---|---|---|
| 1 | Identity and Access Management (IAM) | Identity and Access Management (IAM) |
| 2 | IAM Identity Center | IAM Identity Center |
| 3 | Organizations | Organizations |
| 4 | Resource Access Manager (RAM) | Resource Access Manager (RAM) |

# 5.9 Regions for Using SCPs

SCPs are available in the following regions:

NOTE

Regions for using SCPs also support the use of IAM identity policies.

**Table 5-10** Regions for Using SCPs

| Region Name | Region Code |
|---|---|
| EU-Dublin | eu-west-101 |

# 6 Managing Tag Policies

## 6.1 Overview of a Tag Policy

### Introduction

Tag policies are a type of policy that can help you standardize tags across resources in your organization's accounts. In a tag policy, you specify tagging rules applicable to resources when they are tagged. Untagged resources and tags that are not defined in the tag policy are not evaluated for compliance with the tag policy.

For example, a tag policy can specify that a tag attached to a resource must use the case treatment and tag values defined in the tag policy. If the case and value of the tag do not comply with the tag policy, the resource will be marked as non-compliant.

Currently, tag policies can be used as preventive governance policies. Specifically, if enforcement is enabled for a tag policy, non-compliant tagging operations will be prevented from being performed on specified resource types.

You can attach tag policies to the root OU, other OUs, and accounts within your organization. When you attach a tag policy to the root OU and other OUs, all their child OUs and member accounts inherit that tag policy. The effective tag policy for an account specifies the tagging rules that apply to the account. It is the combination of tag policies that account inherits and tag policies directly attached to that account.

### Functions

**Managing tag policies**

You can create, update, delete, attach, or detach tag policies. OUs and accounts inherit tag policies from one or more of their parent nodes (such as parent OUs). The inherited tag policies are aggregated with those directly attached to the OUs and accounts to form the effective tag policy.

# 6.2 Tag Policy Syntax

## Basic Syntax

The following tag policy shows basic tag policy syntax:

```
{
    "tags": {
        "costcenter": {                 <!-- policy key -->
            "tag_key": {
                "@@assign": "CostCenter"                 <!-- tag key -->
            },
            "tag_value": {
                "@@assign": [
                    "100",                <!-- policy value -->
                    "200"
                ]
            },
            "enforced_for": {                <!-- enforcement -->
                "@@assign": [
                    "apig:instance"                <!-- service or resource type -->
                ]
            }
        }
    }
}
```

- Policy key: A policy key uniquely identifies a policy statement. It must match the value for the tag key, except for the case treatment.
- Tag key: The value for the tag key must match the value for the policy key. But since the policy key value is case insensitive, the capitalization can be different. If the tag key is not defined, lowercase is the default case treatment for tag keys. In this example, **costcenter** is the policy key and **CostCenter** is the tag key, and **CostCenter** is the case treatment that is required for compliance with the tag policy. If the policy key is set to **CostCenter** and the tag key is not defined, the lowercase **costcenter** will be the case treatment required for tag compliance evaluation.
- Policy value: A list of one or more acceptable tag values for the tag key. If you do not specify tag values for a tag key, any value (including no value at all) is considered compliant.
- Enforcement: An **enforced_for** field indicates whether to prevent any non-compliant tagging operations on specified services and resources. If you do not specify any services or resource types in a tag policy, the tag policy will not apply to any resources.
- Wildcard: You can use the wildcard (*) in tag values and the **enforced_for** field provided that you adhere to the following rules:
  - You can use only one wildcard for each tag value. For example, ***@example.com** is allowed, but ***@*.com** is not.
  - For the **enforced_for** field, you can use **<service>:*** to enable enforcement for all resources for a service, but you cannot use a wildcard to specify all services or specify a resource of all services.

## Inheritance Operators

In the preceding example tag policy, the operator @@assign used in the tag key, tag value, and enforcement is an inheritance operator.

Inheritance operators specify how directly attached tag policies and inherited tag policies are merged into the account's effective tag policy. Such operators include value-setting operators and child control operators.

- **Value-setting operators**

  You can use the following value-setting operators to control how your policy interacts with its parent policies.

  **Table 6-1** Value-setting operators

  | Operator | Description |
  |---|---|
  | @@assign | Overwrites any inherited policy settings with the specified setting. If the specified setting is not inherited, this operator adds it to the effective tag policy. This operator can apply to any policy setting of any type.<br>For single-valued settings, this operator replaces the inherited value with the specified value.<br>For multi-valued settings (JSON arrays), this operator removes all inherited values and replaces them with the values specified for this policy. |
  | @@append | Adds the specified settings to the inherited settings, without deleting any settings. If the specified setting is not inherited, this operator adds it to the effective tag policy. You can only use this operator with multi-valued settings.<br>This operator adds the specified value to any values in the inherited array. |
  | @@remove | Removes the specified inherited setting (if there is one) from the effective policy. You can only use this operator with multi-valued settings.<br>This operator removes only the specified values from the array of values inherited from the parent policies. Other values can be retained in the array and inherited by child policies. |

- **Child control operators**

  Child control operators specify which value-setting operators child OUs and accounts can use in child policies. By default, all operators (@@all) are allowed.

  - "@@operators_allowed_for_child_policies":["@@all"] indicates that child OUs and accounts can use any operator in policies. By default, all operators are allowed in child policies.
  - "@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"] indicates that child OUs and accounts can use only the

specified operators in child policies. You can specify one or more value-setting operators in this child control operator.

- "@@operators_allowed_for_child_policies":["@@none"] indicates that child OUs and accounts cannot use operators in policies. You can use this operator to effectively lock the values defined in a parent policy so that the child policies cannot add, append, or delete those values.

# 6.3 Enabling or Disabling the Tag Policy Type

You can enable or disable the tag policy type from the organization' management account, but not from any delegated administrator.

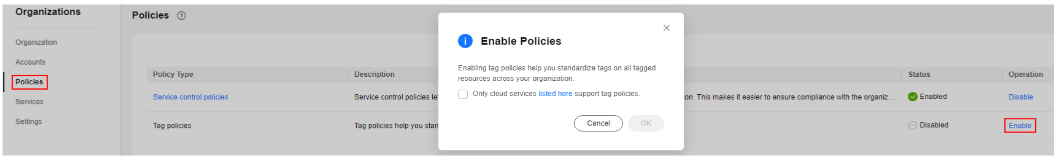
## Enabling the Tag Policy Type

Before you can create and attach tag policies to the OUs and accounts in your organization, you must enable the tag policy type. The only way to enable the tag policy type is by using the organization's management account.

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Policies** page, click **Enable** in the **Operation** column of tag policies.

**Figure 6-1** Enabling the tag policy type



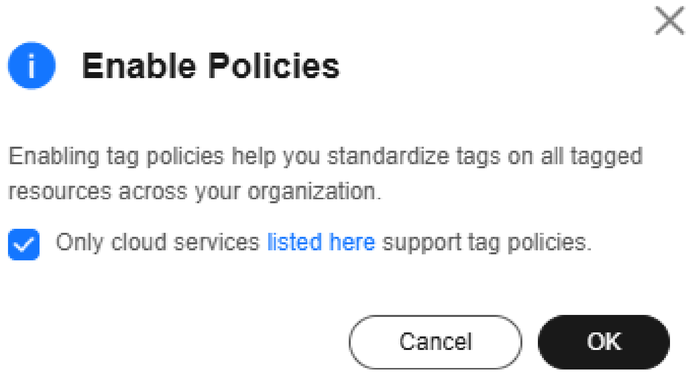
| Policy Type | Description | Status | Operation |
|---|---|---|---|
| Service control policies | Service control policies le… …on. This makes it easier to ensure compliance with the organiz… | Enabled | Disable |
| Tag policies | Tag policies help you stan… | Disabled | Enable |

Enable Policies

Enabling tag policies help you standardize tags on all tagged resources across your organization.

□ Only cloud services listed here support tag policies.

**Step 3** In the displayed dialog box, select the check box and click **OK**.



Enable Policies

Enabling tag policies help you standardize tags on all tagged resources across your organization.

☑ Only cloud services listed here support tag policies.

**----End**

## Disabling the Tag Policy Type

If you no longer want to use tag policies in your organization, you can disable the tag policy type only from the organization's management account.

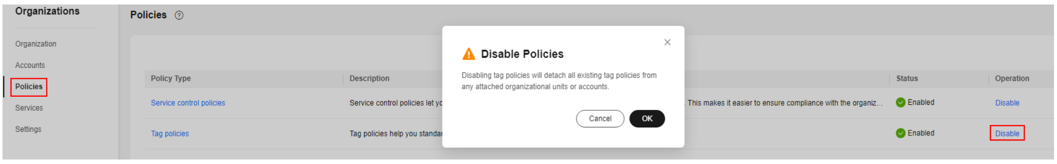
⚠ CAUTION

- After the tag policy type is disabled in an organization, all tag policies are automatically detached from all OUs and accounts in the organization. However, the policies are not deleted.
- If you disable the tag policy type, attachments of tag policies to entities will be lost. If you later re-enable the tag policy type, you must use the management account to re-attach tag policies to the entities.

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Policies** page, click **Disable** in the **Operation** column of tag policies.

**Figure 6-2** Disabling the tag policy type



⚠ Disable Policies

Disabling tag policies will detach all existing tag policies from any attached organizational units or accounts.

| Policy Type | Description | Status | Operation |
|---|---|---|---|
| Service control policies | Service control policies let yo… This makes it easier to ensure compliance with the organiz... | ✓ Enabled | Disable |
| Tag policies | Tag policies help you standar… | ✓ Enabled | Disable |

**Step 3** Click **OK** in the displayed dialog box.

**----End**

# 6.4 Creating a Tag Policy

To standardize the usage of tags in your organization, you can create a tag policy to formulate tag rules.

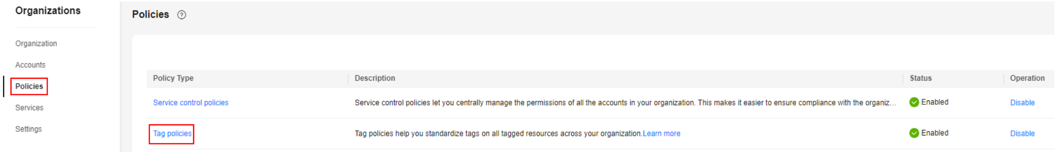
You can create a tag policy from the organization administrator, but not from any delegated administrator.

## Procedure

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** Access the **Policies** page, and click **Tag policies**.

**Figure 6-3** Accessing the **Tag policies** page



| Policy Type | Description | Status | Operation |
|---|---|---|---|
| Service control policies | Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it easier to ensure compliance with the organiz... | ✓ Enabled | Disable |
| Tag policies | Tag policies help you standardize tags on all tagged resources across your organization.Learn more | ✓ Enabled | Disable |

**Step 3** Click **Create Policy**.

**Step 4** Edit the policy name. The policy name is automatically generated when you create a policy, but you can change the policy name if needed. Ensure that you are entering a unique policy name. It must be different from any other existing policy.

(Optional) You can also enter a description for the policy.

**Step 5** Edit the policy content. Currently, you can edit the policy content using the visual editor or JSON.

- Visual editor: When you use the visual editor to edit a policy, you do not need to understand the JSON syntax. After you edit in the visual editor, the new policy is generated automatically. The procedure is as follows:

  a. Enter the key for the tag you want to define in the tag policy.

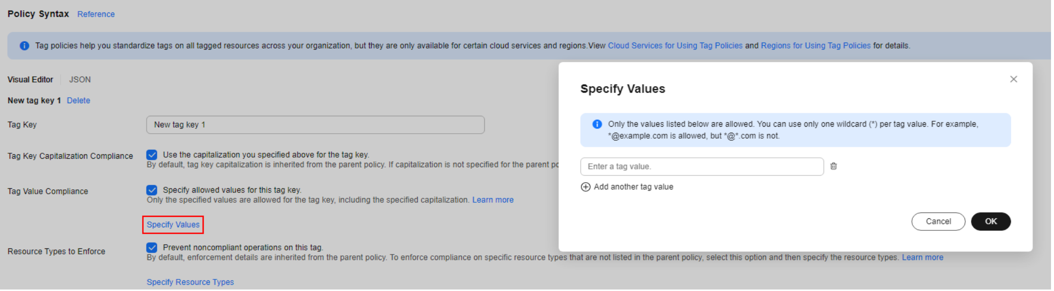
  b. Use the capitalization you specified above for the tag key.

     If you select this option, the capitalization you specified for **Tag Key** is used for checking compliance. If you do not select this option, tag keys in all lowercase characters are considered compliant even if **Tag Key** contains uppercase characters. For example, when you enter **CostCenter** for **Tag Key**, if you select this option, **CostCenter** will be the standard for compliance check; if you do not select this option, **costcenter** will be the standard.

  c. Specify allowed values for this tag key.

     If you select this option and click **Specify Values** to specify one or more allowed values for the tag key, only those values you specified are considered compliant. If you do not select this option or you select this option but do not specify any values, any value (including no value at all) is considered compliant.

     **Figure 6-4** Specifying allowed values for this tag key



Policy Syntax Reference

Tag policies help you standardize tags on all tagged resources across your organization, but they are only available for certain cloud services and regions.View Cloud Services for Using Tag Policies and Regions for Using Tag Policies for details.

Visual Editor | JSON

New tag key 1 Delete

Tag Key: New tag key 1

Tag Key Capitalization Compliance: ☑ Use the capitalization you specified above for the tag key.
By default, tag key capitalization is inherited from the parent policy. If capitalization is not specified for the parent po

Tag Value Compliance: ☑ Specify allowed values for this tag key.
Only the specified values are allowed for the tag key, including the specified capitalization. Learn more

Specify Values

Resource Types to Enforce: ☑ Prevent noncompliant operations on this tag.
By default, enforcement details are inherited from the parent policy. To enforce compliance on specific resource types that are not listed in the parent policy, select this option and then specify the resource types. Learn more

Specify Resource Types

Specify Values

Only the values listed below are allowed. You can use only one wildcard (*) per tag value. For example, *@example.com is allowed, but *@*.com is not.

Enter a tag value.

Add another tag value

Cancel OK

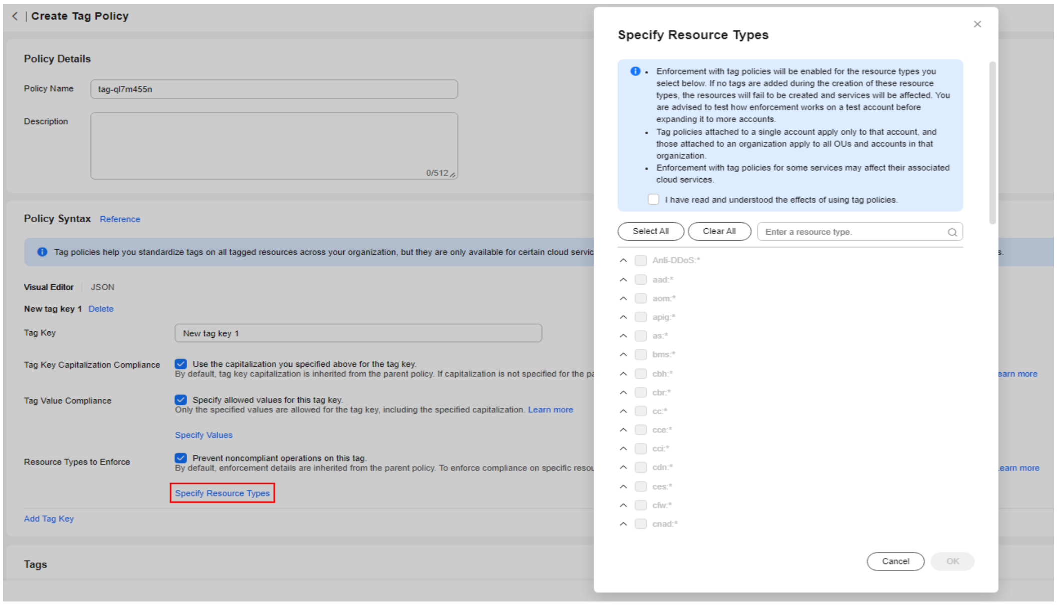
  d. Specify resource types to enforce the tag policy.

     Select the **Prevent noncompliant operations on this tag.** option and click **Specify Resource Types**. In the displayed dialog box, read and confirm the effects of using tag policies. Then, select resource types and click **OK**.

     NOTE

     If you do not specify any services or resource types, the tag policy will not apply to any resources.

**Figure 6-5** Specifying resource types



< | **Create Tag Policy**

**Policy Details**

Policy Name: tag-ql7m455n

Description: 0/512

**Policy Syntax** Reference

Tag policies help you standardize tags on all tagged resources across your organization, but they are only available for certain cloud servic

**Visual Editor** | JSON

**New tag key 1** Delete

Tag Key: New tag key 1

Tag Key Capitalization Compliance: ☑ Use the capitalization you specified above for the tag key.
By default, tag key capitalization is inherited from the parent policy. If capitalization is not specified for the pa

Tag Value Compliance: ☑ Specify allowed values for this tag key.
Only the specified values are allowed for the tag key, including the specified capitalization. Learn more

Specify Values

Resource Types to Enforce: ☑ Prevent noncompliant operations on this tag.
By default, enforcement details are inherited from the parent policy. To enforce compliance on specific resou

Specify Resource Types

Add Tag Key

**Tags**

**Specify Resource Types** ×

- Enforcement with tag policies will be enabled for the resource types you select below. If no tags are added during the creation of these resource types, the resources will fail to be created and services will be affected. You are advised to test how enforcement works on a test account before expanding it to more accounts.
- Tag policies attached to a single account apply only to that account, and those attached to an organization apply to all OUs and accounts in that organization.
- Enforcement with tag policies for some services may affect their associated cloud services.

□ I have read and understood the effects of using tag policies.

Select All | Clear All | Enter a resource type.

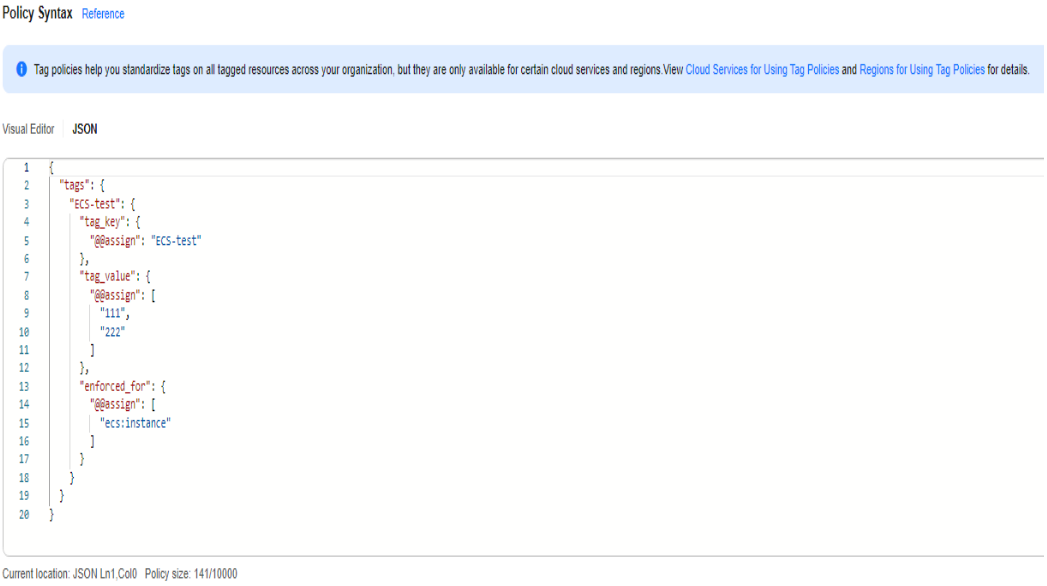
□ Anti-DDoS:*
□ aad:*
□ aom:*
□ apig:*
□ as:*
□ bms:*
□ cbh:*
□ cbr:*
□ cc:*
□ cce:*
□ cci:*
□ cdn:*
□ ces:*
□ cfw:*
□ cnad:*

Cancel | OK

e. Click **Add Tag Key** to add another tag key to this tag policy.

- JSON: When using JSON syntax, you can edit the policy text by referring to **Tag Policy Syntax**. The system automatically verifies the syntax. If the syntax is incorrect, modify it as prompted.

**Figure 6-6** Editing a policy using JSON



Policy Syntax Reference

Tag policies help you standardize tags on all tagged resources across your organization, but they are only available for certain cloud services and regions. View Cloud Services for Using Tag Policies and Regions for Using Tag Policies for details.

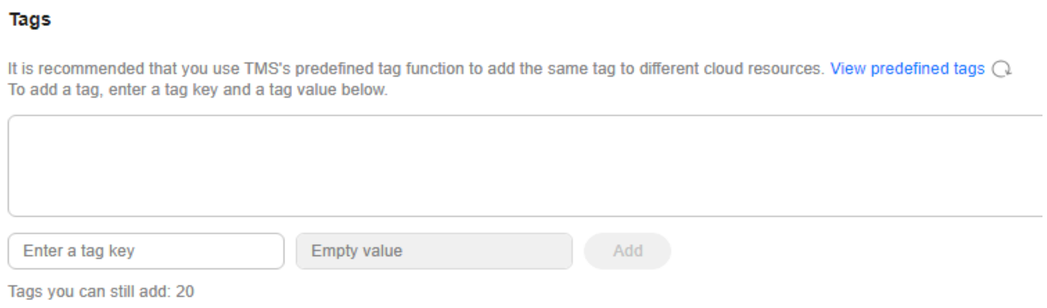
Visual Editor | **JSON**

```
{
  "tags": {
    "ECS-test": {
      "tag_key": {
        "@@assign": "ECS-test"
      },
      "tag_value": {
        "@@assign": [
          "111",
          "222"
        ]
      },
      "enforced_for": {
        "@@assign": [
          "ecs:instance"
        ]
      }
    }
  }
}
```

Current location: JSON Ln1,Col0  Policy size: 141/10000

**Step 6** (Optional) Add one or more tags. Enter a tag key and a tag value, and click **Add**.

**Figure 6-7** Adding a tag



Tags

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags
To add a tag, enter a tag key and a tag value below.

Tags you can still add: 20

**Step 7** Click **Save** in the lower right corner. If the tag policy is created successfully, it will be added to the list.

**----End**

# 6.5 Viewing the Effective Tag Policy

You can attach tag policies to the root OU, other OUs, and accounts within your organization. When you attach a tag policy to the root OU and other OUs, all their child OUs and member accounts inherit that tag policy. The effective tag policy for an account specifies the tagging rules that apply to the account. It is the combination of tag policies that account inherits and tag policies directly attached to that account.

The following describes how a tag policy is prioritized as the effective tag policy:

- Tag policies attached to entities at the same hierarchy level:
  - Single-valued operators: If you attach multiple tag policies, the first policy using the @@assign operator will be considered to be the effective tag policy.
  - Multi-valued operators: If you attach multiple tag policies, the first policy using the @@assign operator will be considered to be the effective tag policy, and the @@append and @@remove operators used by other policies still take effect.
- Tag policies attached to entities at the different hierarchy levels:

  If the upper- and lower-level entities use the same tag key, tag policies are calculated from the upper-level entities to the lower-level entities based on the types of child control operators to comprise the effective tag policy. If the upper and lower levels use different tag keys, the combination of their tag policies comprises the effective tag policy.

To view the effective tag policy for the root OU, other OUs, and accounts of an organization on the management console, use the following procedure:

## Procedure

**Step 1** Log in to the Organizations console on Huawei Cloud and access the **Organization** page.

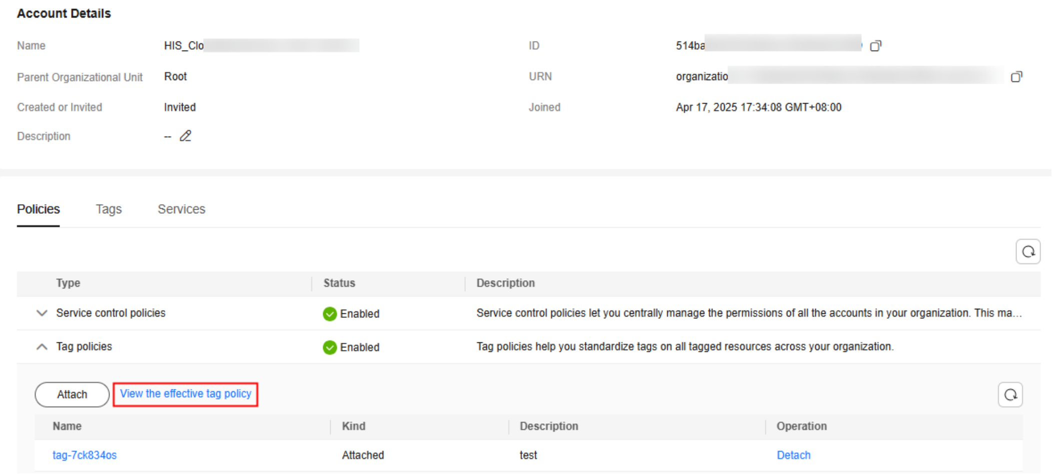
**Step 2** Choose **Organization** in the navigation pane.

**Step 3** Click the root OU, specific OU, or account of your organization. You can view its details on the right of the organization tree.

**Step 4** Click the **Policies** tab.

**Step 5** Expand the tag policy list and click **View the effective tag policy** above the list. The effective tag policy is presented in JSON.

**Figure 6-8** Viewing the effective tag policy



Account Details

Name HIS_Clo[redacted]
ID 514ba[redacted]
Parent Organizational Unit Root
URN organizatio[redacted]
Created or Invited Invited
Joined Apr 17, 2025 17:34:08 GMT+08:00
Description --

| Type | Status | Description |
|---|---|---|
| Service control policies | Enabled | Service control policies let you centrally manage the permissions of all the accounts in your organization. This ma... |
| Tag policies | Enabled | Tag policies help you standardize tags on all tagged resources across your organization. |

| Name | Kind | Description | Operation |
|---|---|---|---|
| tag-7ck834os | Attached | test | Detach |

**----End**

# 6.6 Editing or Deleting a Tag Policy

The following describes how to edit and delete a tag policy.

You can edit or delete a tag policy from the organization administrator, but not from a delegated administrator.

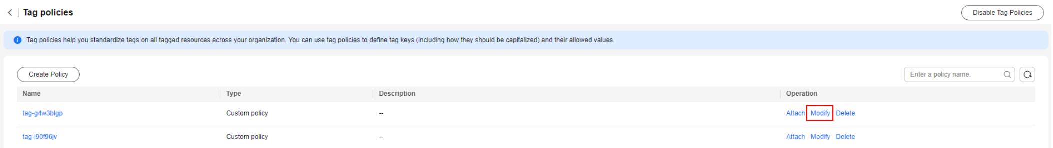
## Editing a Tag Policy

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** Access the **Policies** page, and click **Tag policies**.

**Step 3** Locate the target tag policy and click **Modify** in the **Operation** column. The **Edit Tag Policy** page is displayed.

**Figure 6-9** Editing a tag policy



Tag policies help you standardize tags on all tagged resources across your organization. You can use tag policies to define tag keys (including how they should be capitalized) and their allowed values.

| Name | Type | Description | Operation |
|---|---|---|---|
| tag-g4w3blgp | Custom policy | -- | Attach Modify Delete |
| tag-i90f96jv | Custom policy | -- | Attach Modify Delete |

**Step 4** Enter a new policy name and description.

**Step 5** Edit the policy content if needed. You can choose either visual editor or JSON to edit the policy.

**Step 6** Click **Save** in the lower right corner. If the tag policy is updated successfully, it will be added to the list.

**----End**

## Deleting a Tag Policy

A tag policy that is attached to OUs or accounts cannot be deleted. To delete such a tag policy, you need to detach it from the OUs or accounts first.

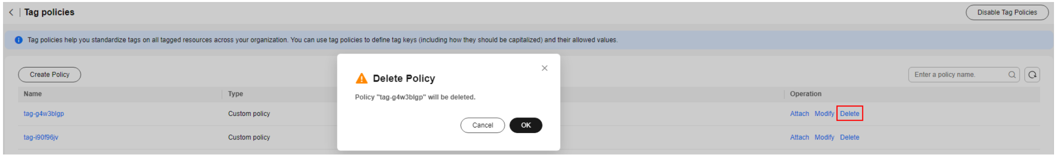
**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** Access the **Policies** page, and click **Tag policies**.

**Step 3** Locate the tag policy you want to delete and click **Delete** in the **Operation** column.

**Step 4** Click **OK** in the displayed dialog box.

**Figure 6-10** Deleting a tag policy



Tag policies help you standardize tags on all tagged resources across your organization. You can use tag policies to define tag keys (including how they should be capitalized) and their allowed values.

Policy "tag-g4w3blgp" will be deleted.

| Name | Type | Operation |
|---|---|---|
| tag-g4w3blgp | Custom policy | Attach Modify Delete |
| tag-i90f96jv | Custom policy | Attach Modify Delete |

**----End**

# 6.7 Attaching or Detaching a Tag Policy

You can attach a tag policy to or detach it from the root OU, other OUs or accounts from the organization's management account.

## Constraints

- You can attach up to 10 tag policies to an account.
- You can attach or detach a tag policy from only the organization administrator, but not from a delegated administrator.
- Tag policies are applied within 30 minutes after they are attached.

## Attaching a Tag Policy

**Method 1:**

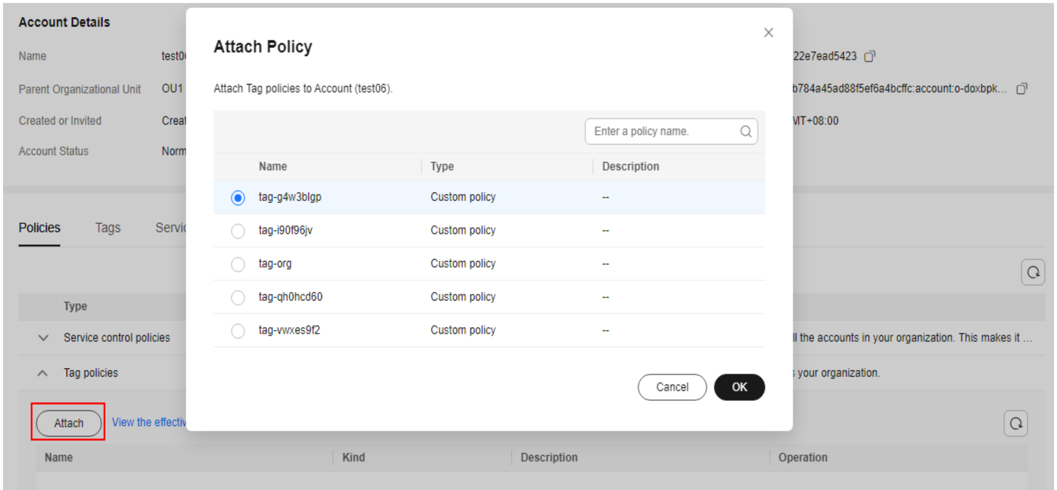
**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the OU or account you want to attach a tag policy to.

**Step 3** On the details page, click the **Policies** tab. On the page, expand **Tag policies** and click **Attach**.

**Step 4** Select the tag policy you want to attach and click **OK**.

**Figure 6-11** Attaching a tag policy



Attach Policy

Attach Tag policies to Account (test06).

| | Name | Type | Description |
|---|---|---|---|
| ● | tag-g4w3blgp | Custom policy | -- |
| ○ | tag-i90f96jv | Custom policy | -- |
| ○ | tag-org | Custom policy | -- |
| ○ | tag-qh0hcd60 | Custom policy | -- |
| ○ | tag-vwxes9f2 | Custom policy | -- |

----End

**Method 2:**

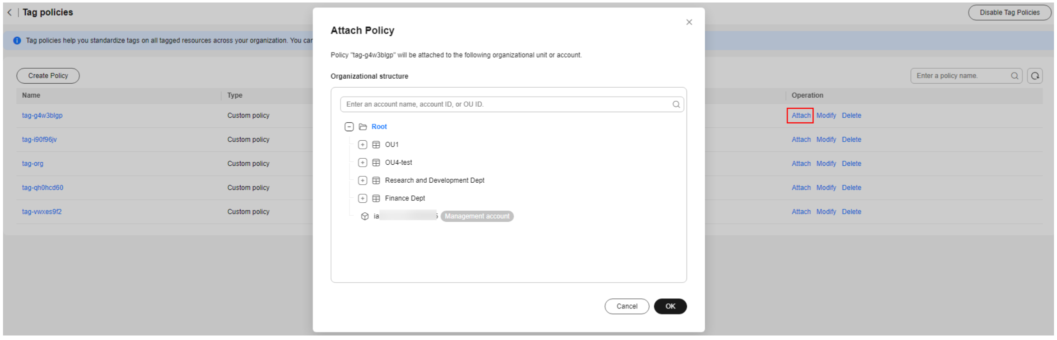
**Step 1** Access the **Policies** page on the Organizations console.

**Step 2** Click **Tag policies**. The list of tag policies is displayed.

**Step 3** Locate the tag policy you want to attach and click **Attach** in the **Operation** column. Then, select the OU or account you want to attach the policy to.

**Step 4** Click **OK**.

**Figure 6-12** Attaching a tag policy



Tag policies

Tag policies help you standardize tags on all tagged resources across your organization. You car

| Name | Type | Operation |
|---|---|---|
| tag-g4w3blgp | Custom policy | Attach Modify Delete |
| tag-i90f96jv | Custom policy | Attach Modify Delete |
| tag-org | Custom policy | Attach Modify Delete |
| tag-qh0hcd60 | Custom policy | Attach Modify Delete |
| tag-vwxes9f2 | Custom policy | Attach Modify Delete |

Attach Policy

Policy "tag-g4w3blgp" will be attached to the following organizational unit or account.

Organizational structure

- Root
  - OU1
  - OU4-test
  - Research and Development Dept
  - Finance Dept
  - ia[redacted] Management account

----End

## Detaching a Tag Policy

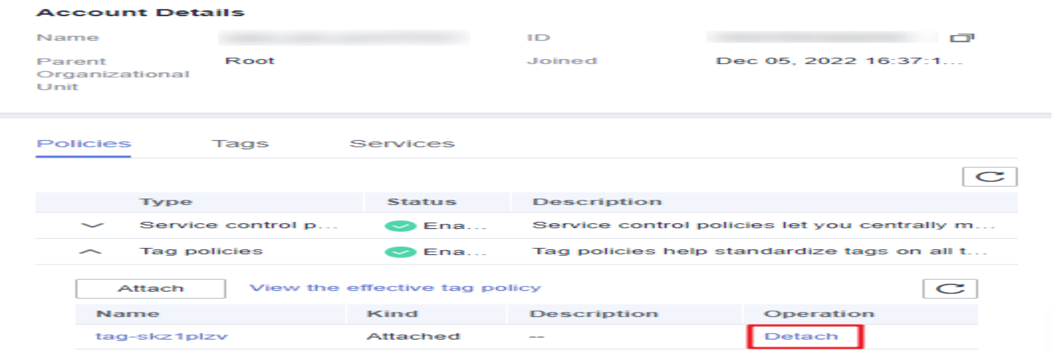
**Method 1:**

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the OU or account you want to detach a tag policy from.

**Step 3** On the details page, click the **Policies** tab. On the page, expand **Tag policies**, locate the target tag policy and click **Detach** in the **Operation** column.

**Figure 6-13** Detaching a tag policy



Account Details

Name [redacted] ID [redacted]

Parent Organizational Unit Root Joined Dec 05, 2022 16:37:1...

| | Type | Status | Description |
|---|---|---|---|
| ﹀ | Service control p... | Ena... | Service control policies let you centrally m... |
| ︿ | Tag policies | Ena... | Tag policies help standardize tags on all t... |

| Name | Kind | Description | Operation |
|---|---|---|---|
| tag-skz1plzv | Attached | -- | Detach |

**Step 4** Click **Detach** in the displayed dialog box.

**----End**

**Method 2:**

**Step 1** Access the **Policies** page on the Organizations console.

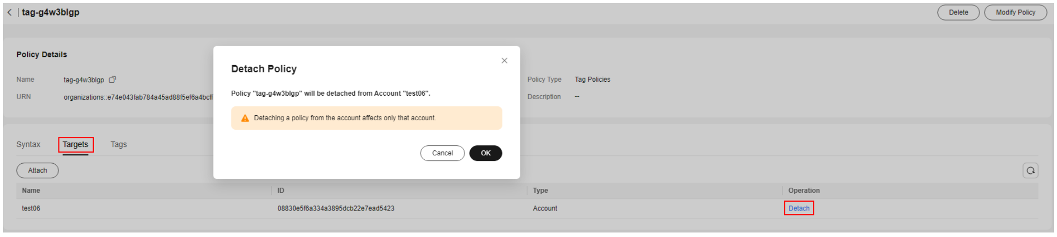
**Step 2** Click **Tag policies**. The list of tag policies is displayed.

**Step 3** Click the name of the target tag policy and click the **Targets** tab.

**Step 4** Locate the OU or account that you want to detach the tag policy from and click **Detach** in the **Operation** column.

**Step 5** Click **OK**.

**Figure 6-14** Detaching a tag policy



Policy Details

Name tag-g4w3blgp

URN organizations::e74e043fab784a45ad88f5ef6a4bcff

Policy Type Tag Policies

Description --

Detach Policy

Policy "tag-g4w3blgp" will be detached from Account "test06".

Detaching a policy from the account affects only that account.

| Name | ID | Type | Operation |
|---|---|---|---|
| test06 | 08830e5f6a334a3895dcb22e7ead5423 | Account | Detach |

**----End**

## 6.8 Cloud Services for Using Tag Policies

Tag policies are available for the following cloud services and resource types:

**Table 6-2** Supported cloud services and resources types

| Service Name | Resource Type |
|---|---|
| Auto Scaling (AS) | Scaling groups |
| Bare Metal Server (BMS) | Instances |
| Cloud Bastion Host (CBH) | Instances |
| Cloud Backup and Recovery (CBR) | Vaults |
| Cloud Container Engine (CCE) | Clusters |
| Cloud Secret Management Service (CSMS) | Secret |
| Cloud Search Service (CSS) | ● Clusters<br>● Log stream<br>● Repository |
| Cloud Trace Service (CTS) | Trackers |
| DataArts Studio | ● Instances<br>● Workspace |
| Database Security Service (DBSS) | Audit instances |
| Direct Connect | ● Direct connections<br>● Global DC gateways<br>● Lag<br>● Virtual gateways<br>● Virtual interfaces |
| Distributed Cache Service (DCS) | Instances |
| Document Database Service (DDS) | Instance names |
| Data Lake Insight (DLI) | ● Databases<br>● Enhanced datasource connections<br>● Elastic resource pools<br>● Jobs<br>● Queues<br>● Resources |
| Distributed Message Service (DMS) | ● Kafka instances<br>● RabbitMQ instances<br>● RocketMQ instances |
| Domain Name Service (DNS) | ● PTR<br>● Domain names |
| Data Replication Service (DRS) | Jobs |

| Service Name | Resource Type |
|---|---|
| Data Warehouse Service (DWS) | Clusters |
| Elastic Cloud Server (ECS) | Instances |
| Elastic Load Balance (ELB) | ● Listeners<br>● Load balancers |
| Enterprise Router | ● Attachments<br>● Instances<br>● Route tables |
| Elastic Volume Service (EVS) | Volume |
| FunctionGraph | Functions |
| Identity and Access Management (IAM) | ● Agencies<br>● Users |
| Image Management Service (IMS) | Images |
| Key Management Service (KMS) | Customer master keys |
| Log Tank Service (LTS) | ● Log access configuration<br>● Host groups<br>● Log groups<br>● Log stream |
| ModelArts | ● Notebook<br>● Resource pools<br>● Services<br>● Training jobs |
| MapReduce Service (MRS) | Clusters |
| NAT Gateway | ● Public gateways<br>● Private gateways<br>● Private transit IP addresses<br>● Transit subnets |
| Organizations | ● Accounts<br>● Organizational units<br>● Policies<br>● Root |
| Resource Access Manager (RAM) | Resource shares |
| Relational Database Service (RDS) | Instances |
| SecMaster | Workspace |
| Simple Message Notification (SMN) | Topics |

| Service Name | Resource Type |
|---|---|
| Virtual Private Cloud (VPC) | ● Public IP addresses<br>● Subnets<br>● VPC<br>● Network ACLs (firewalls)<br>● Security groups |
| VPC Endpoint (VPCEP) | ● Endpoint services<br>● Endpoints |
| IAM Identity Center | ● Permission setting |
| Elastic IP (EIP) | ● Global EIP<br>● Global Internet Bandwidth |

## 6.9 Regions for Using Tag Policies

Tag policies are available in the following regions:

**Table 6-3** Supported regions

| Region Name | Region Code |
|---|---|
| EU-Dublin | eu-west-101 |

# 7 Managing Trusted Services

## 7.1 Overview of a Trusted Service

### What Is a Trusted Service?

You can use the management account in Organizations to enable trusted access for a supported Huawei Cloud service, called a trusted service. A trusted service can perform tasks in your organization on your behalf. Each trusted service has access to the information about the OUs and member accounts in your organization and also can manage the entire organization. For example, if you enable CTS as a trusted service for Organizations, CTS can obtain information about OUs and member accounts to record the operations in all accounts within the organization. For cloud services that can be enabled with trusted access, see **Trusted Services for Organizations**.

### Delegated Administrator

A delegated administrator account is a member account that has special permissions in an organization. The management account of your organization can designate a member account to be a delegated administrator account for a trusted service. All the users in the delegated administrator account will have organizational management capabilities. For example, if a member account becomes the delegated administrator of CTS, the account can view the CTS logs of all member accounts in the organization.

### Service-linked Agency

The Organizations service uses IAM trust agencies to enable trusted services to perform tasks on your behalf in your organization's member accounts. When you enable a trusted service, the service can request that Organizations create a service-linked agency in its member accounts. The trusted service does this asynchronously, as needed. The service-linked agency has predefined IAM permissions that allow the trusted service to perform specific tasks within that account. This means that the capabilities of that cloud service are extended to the entire multi-account organization. For details about the supported trusted services and their functions, see **Trusted Services for Organizations**.

When you create an account in your organization or invite an existing account to join your organization, Organizations provisions the member account with a service-linked agency with the system-defined permission **OrganizationsServiceLinkedAgencyPolicy**, which is applicable to all resources. Only the Organizations service itself can assume this agency. This agency has permission that allows Organizations to create service-linked agencies for other cloud services.

**NOTE**

Organizations SCPs do not affect service-linked agencies, and operations performed using service-linked agencies are not restricted by SCPs.

# 7.2 Enabling or Disabling a Trusted Service

- If the organization administrator disables trusted access for a cloud service, the service can no longer create a service-linked agency in the member accounts.
- If the organization administrator closes the organization or a member account leaves the organization, Organizations will clear its service-linked agency.
- Before disabling trusted access for the AOM service, delete multi-account instances on the AOM console and then disable the trusted access on the Organizations console. Otherwise, the multi-account instances will continue retrieving the member accounts' metric data.
- Before disabling trusted access for the LTS service, delete the configurations of multi-account log aggregation on the LTS console and then disable the trusted access on the Organizations console. Otherwise, the multi-account log aggregation will continue retrieving the member accounts' logs.

## Enabling a Trusted Service

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Services** page, locate the target trusted service and click **Enable Access** in the **Operation** column.

**Step 3** Click **OK** in the displayed dialog box.

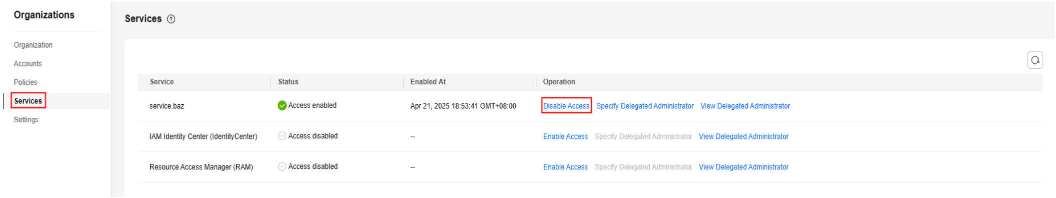
**----End**

## Disabling a Trusted Service

When logging in as the organization's management account, you can disable trusted services.

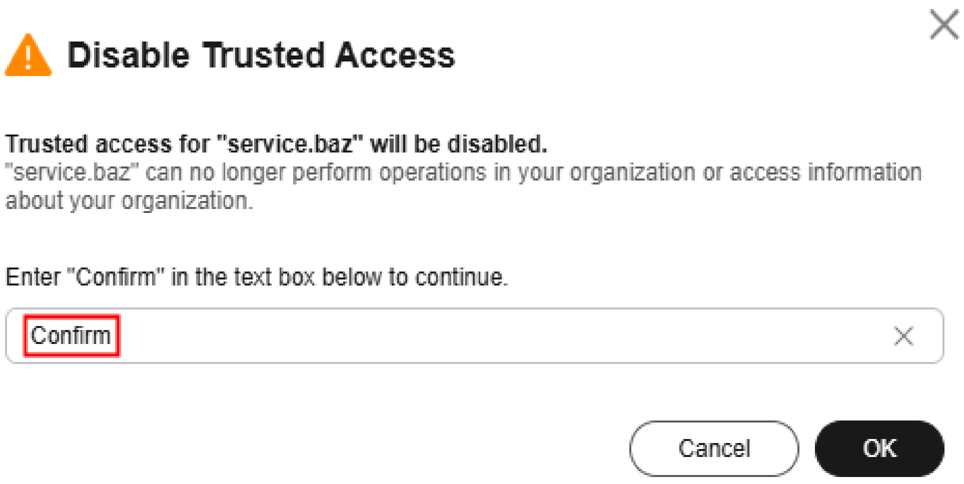
**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Services** page, locate the target trusted service and click **Disable Access** in the **Operation** column.



| Service | Status | Enabled At | Operation |
|---|---|---|---|
| service.baz | ✓ Access enabled | Apr 21, 2025 18:53:41 GMT+08:00 | Disable Access Specify Delegated Administrator View Delegated Administrator |
| IAM Identity Center (IdentityCenter) | ○ Access disabled | -- | Enable Access Specify Delegated Administrator View Delegated Administrator |
| Resource Access Manager (RAM) | ○ Access disabled | -- | Enable Access Specify Delegated Administrator View Delegated Administrator |

**Step 3** In the displayed dialog box, enter "Confirm" and click **OK**.



Disable Trusted Access

Trusted access for "service.baz" will be disabled.
"service.baz" can no longer perform operations in your organization or access information about your organization.

Enter "Confirm" in the text box below to continue.

Confirm

**----End**

## 7.3 Trusted Services for Organizations

Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Services** page to view the trusted services for Organizations.

The following table lists the cloud services that can be used with Huawei Cloud Organizations.

**Table 7-1** Trusted services for Organizations

| Service Name | Benefits of Using with Organizations | Delegated Administrator | Maximum Number of Delegated Administrators | Reference |
|---|---|---|---|---|
| Resource Access Manager (RAM) | You can easily share resources within a given organization. When your account is managed by an organization, you can share resources with all accounts in the organization. Accounts in the same organization can use the shared resources without being invited. | Supported | Unlimited | **Enabling Sharing with Organizations** |

| Service Name | Benefits of Using with Organizations | Delegated Administrator | Maximum Number of Delegated Administrators | Reference |
|---|---|---|---|---|
| IAM Identity Center | You can use IAM Identity Center to centrally manage your workforce identities and their access to multiple accounts in your organization. You can create identities for your entire enterprise at one go and give them single sign-on (SSO) access with managed permissions. | Supported | Unlimited | What Is IAM Identity Center? |

# 7.4 Specifying, Viewing, or Removing a Delegated Administrator

NOTICE

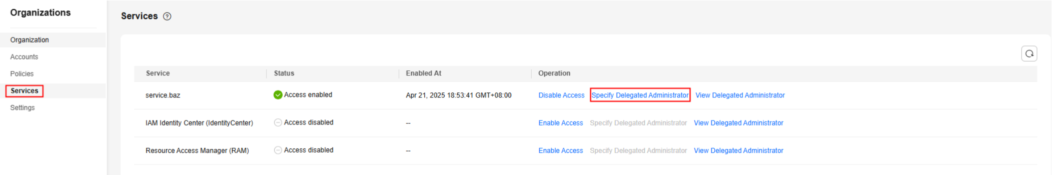
- Before removing the delegated administrator of the trusted service AOM, delete the multi-account instances on the AOM console and then access the Organizations console to start removal. Otherwise, the multi-account instances will continue retrieving the member accounts' metric data.
- Before removing the delegated administrator of the trusted service LTS, delete the configurations of multi-account log aggregation on the LTS console and then access the Organizations console to start removal. Otherwise, the multi-account log aggregation will continue retrieving the member accounts' logs.

## Specifying a Delegated Administrator

An account being closed cannot be specified as a delegated administrator.

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Services** page, locate the target trusted service and click **Specify Delegated Administrator** in the **Operation** column.



| Service | Status | Enabled At | Operation |
|---|---|---|---|
| service.baz | Access enabled | Apr 21, 2025 18:53:41 GMT+08:00 | Disable Access Specify Delegated Administrator View Delegated Administrator |
| IAM Identity Center (IdentityCenter) | Access disabled | -- | Enable Access Specify Delegated Administrator View Delegated Administrator |
| Resource Access Manager (RAM) | Access disabled | -- | Enable Access Specify Delegated Administrator View Delegated Administrator |

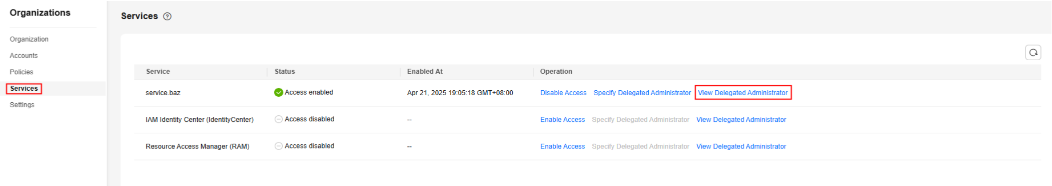
**Step 3** Select the account to be specified as the delegated administrator, and click **OK**.

**----End**

## Viewing a Delegated Administrator

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Services** page, locate the target trusted service and click **View Delegated Administrator** in the **Operation** column.



| Service | Status | Enabled At | Operation |
|---|---|---|---|
| service.baz | Access enabled | Apr 21, 2025 19:05:18 GMT+08:00 | Disable Access Specify Delegated Administrator View Delegated Administrator |
| IAM Identity Center (IdentityCenter) | Access disabled | -- | Enable Access Specify Delegated Administrator View Delegated Administrator |
| Resource Access Manager (RAM) | Access disabled | -- | Enable Access Specify Delegated Administrator View Delegated Administrator |

**Step 3** View the details about the delegated administrator of the trusted service.

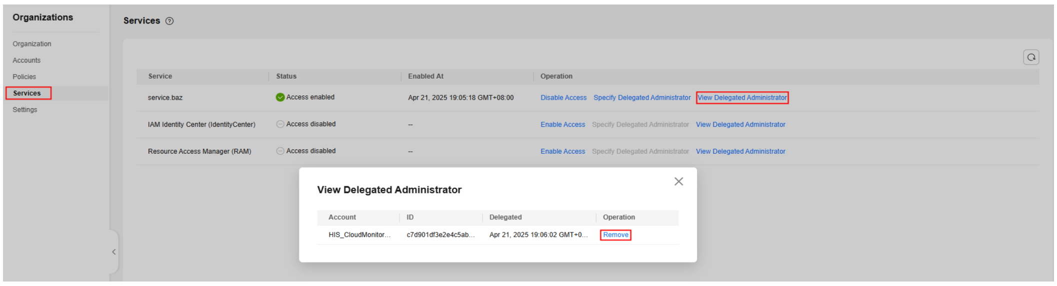
**----End**

## Removing a Delegated Administrator

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Services** page, locate the target trusted service and click **View Delegated Administrator** in the **Operation** column.

**Step 3** In the displayed dialog box, click **Remove** in the **Operation** column.



| Service | Status | Enabled At | Operation |
|---|---|---|---|
| service.baz | Access enabled | Apr 21, 2025 19:05:18 GMT+08:00 | Disable Access Specify Delegated Administrator View Delegated Administrator |
| IAM Identity Center (IdentityCenter) | Access disabled | -- | Enable Access Specify Delegated Administrator View Delegated Administrator |
| Resource Access Manager (RAM) | Access disabled | -- | Enable Access Specify Delegated Administrator View Delegated Administrator |

View Delegated Administrator

| Account | ID | Delegated | Operation |
|---|---|---|---|
| HIS_CloudMonitor... | c7d901df3e2e4c5ab... | Apr 21, 2025 19:06:02 GMT+0... | Remove |

**Step 4** Click **OK** in the displayed dialog box.

**----End**

# 8 Managing Tags

## 8.1 Overview of a Tag

### Tag Introduction

A tag is a custom label you use to identify, categorize, and search for cloud resources. You can add tags to the following organization resources:

- Organization root
- Organizational units (OUs)
- Accounts
- Service control policies (SCPs)
- Tag policies

You can add tags at the following times:

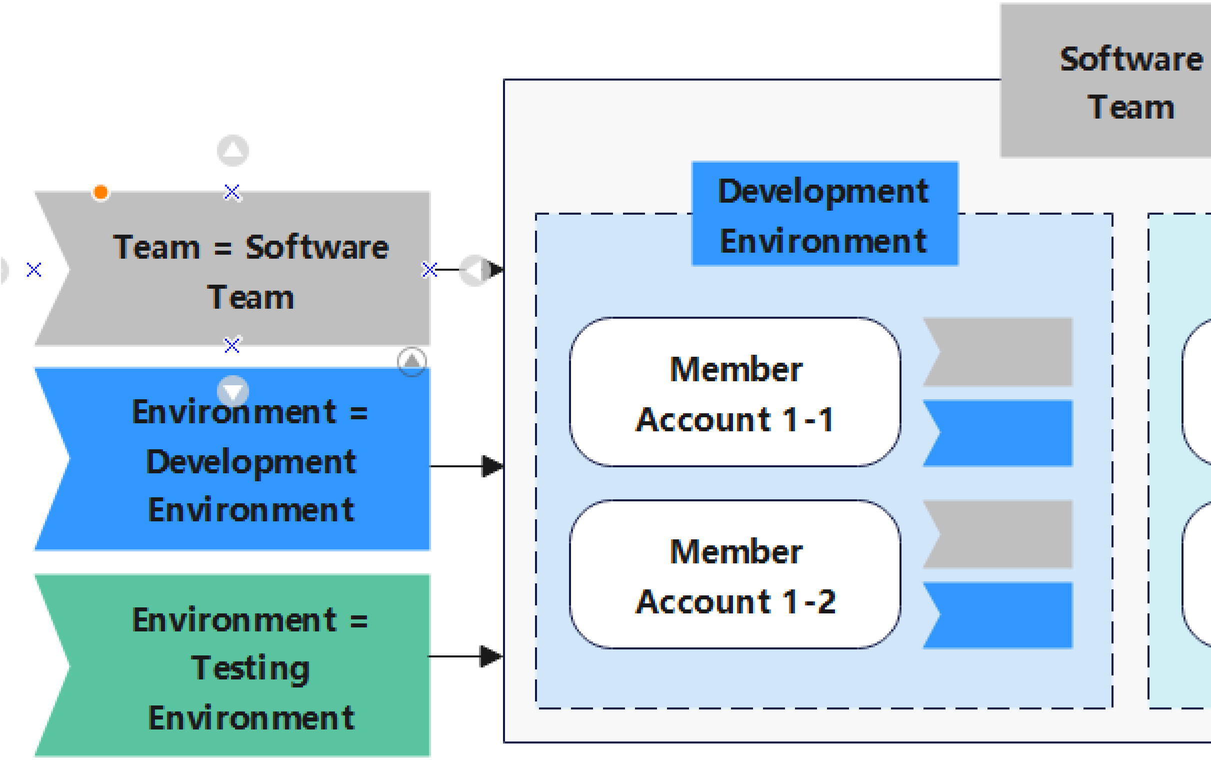
- When you create OUs, accounts, SCPs, or tag policies, you can add tags.
- When you view details about the organization root, OUs, accounts, SCPs, or tag policies, you can add, update, view, or delete tags on their details pages.

### Basics of Tags

Tags help you to identify your cloud resources. When you have many cloud resources of the same type, you can use tags to classify them by dimension (for example, use, owner, or environment).

**Figure 8-1** shows an example of how tags work. In this example, two tags were assigned to each member account. Each tag contains a key and a value defined by the user. The key of one tag is **Team**, and the key of another tag is **Environment**.

**Figure 8-1** Example of tags



You can quickly search for and filter specific cloud resources based on the tags added to them. For example, you can define a set of tags for cloud resources in an account to track the owner and usage of each cloud resource, making resource management easier and faster.

## Constraints on Using Tags

- The following basic naming and usage requirements apply to the key and value of a tag:

  Tag key:

  – Cannot be an empty string.

  – Contains 1 to 128 characters.

  – Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF).

  Tag value:

  – Can be an empty string.

  – Contains 1 to 225 characters.

  – Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF).

- Each cloud resource can have a maximum of 20 tags.
- For each resource, each tag key must be unique and can have only one tag value.

Helpful links:

- **Adding a Tag**: You can add tags for your OUs, accounts, SCPs, and tag policies.
- **Editing a Tag**: You can update the tag keys and values for OUs, accounts, SCPs, and tag policies.
- **Viewing Tag Details**: You can view the tags attached to OUs, accounts, SCPs, and tag policies.
- **Deleting a Tag**: You can delete tags from OUs, accounts, SCPs, and tag policies.

# 8.2 Adding a Tag

## 8.2.1 Adding a Tag for the Root, OUs, or Accounts

### Scenario

The following describes how to add a tag for the root, OUs, or accounts.

### Procedure

You add tags to the root, OUs, and accounts in the same way. The following uses adding tags to an OU as an example.

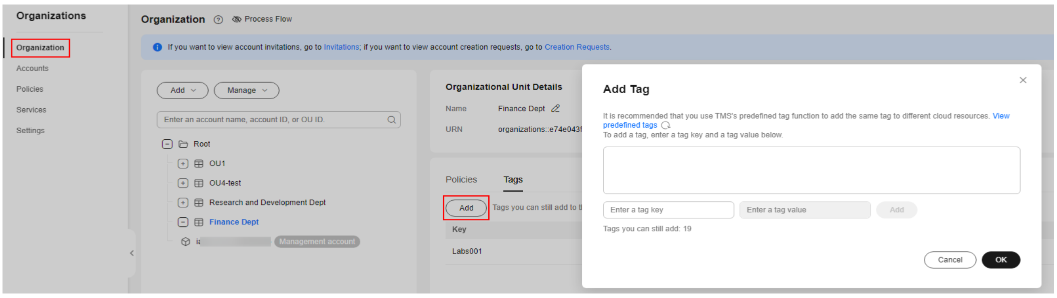
**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the OU you want to add a tag to, click the **Tags** tab in the pane on the right, and click **Add**.

**Step 3** Enter a tag key and a tag value, click **Add**, and click **OK**.

You can select a predefined tag created in TMS from the drop-down lists. For details, see **Creating Predefined Tags**.

**Figure 8-2** Adding a tag



If you want to view account invitations, go to Invitations; if you want to view account creation requests, go to Creation Requests.

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

To add a tag, enter a tag key and a tag value below.

Tags you can still add: 19

**----End**

## 8.2.2 Adding a Tag for a Policy

### Scenario

The following describes how to add a tag from custom SCPs and tag policies.

### Procedure

The procedures for adding tags to SCPs and tag policies are similar. The following uses how to add tags to custom SCPs as an example.

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Policies** page, click **Service control policies**.

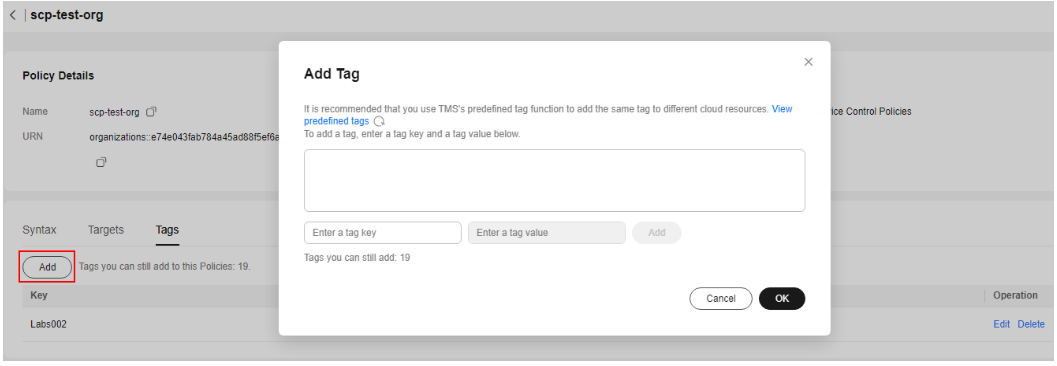
**Step 3** Click the name of a policy to go to the policy details page.

**Step 4** Click the **Tags** tab, and then click **Add**.

**Step 5** Enter a tag key and a tag value, click **Add**, and click **OK**.

You can select a predefined tag created in TMS from the drop-down lists. For details, see **Creating Predefined Tags**.

**Figure 8-3** Adding a tag



It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

To add a tag, enter a tag key and a tag value below.

Tags you can still add: 19

Tags you can still add to this Policies: 19.

Name: scp-test-org

URN: organizations::e74e043fab784a45ad88f5ef6a

| Key | Operation |
|---|---|
| Labs002 | Edit Delete |

**----End**

# 8.3 Editing a Tag

## 8.3.1 Editing a Tag for the Root, OUs, or Accounts

### Scenario

The following describes how to edit a tag for the root, OUs, or accounts.

### Procedure

You edit tags for the root, OUs, and accounts in the same way. The following uses editing tags for an OU as an example.

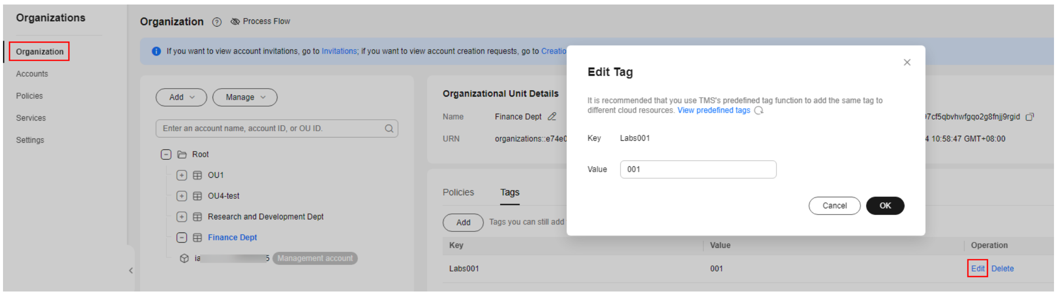
**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the OU you want to update a tag to, and click the **Tags** tab in the pane on the right. The list of tags is displayed.

**Step 3** Locate the tag you want to edit and click **Edit** in the **Operation** column.

**Step 4** Enter a new tag value, and click **OK** in the displayed dialog box.

**Figure 8-4** Editing a tag



If you want to view account invitations, go to Invitations; if you want to view account creation requests, go to Creatio

Enter an account name, account ID, or OU ID.

Name Finance Dept

URN organizations::e74e0

7cf5qbvhwfgqo2g8fnjj9rgid

4 10:58:47 GMT+08:00

Tags you can still add

Edit Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Key Labs001

Value 001

Cancel OK

| Key | Value | Operation |
|---|---|---|
| Labs001 | 001 | Edit Delete |

**----End**

# 8.3.2 Editing a Tag for a Policy

## Scenario

The following describes how to edit a tag from custom SCPs and tag policies.

## Procedure

The procedures for editing tags for SCPs and tag policies are similar. The following uses how to edit tags for custom SCPs as an example.

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

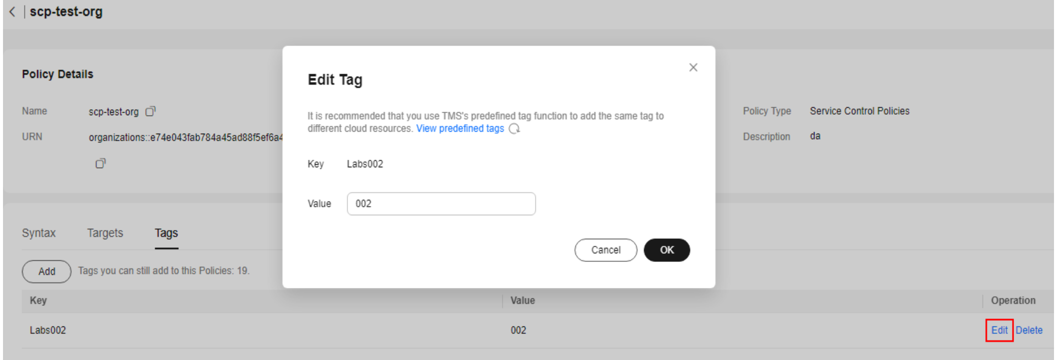
**Step 2** On the **Policies** page, click **Service control policies**.

**Step 3** Click the name of a policy to go to the policy details page.

**Step 4** On the **Tags** page, locate the tag you want to edit and click **Edit** in the **Operation** column.

**Step 5** Enter a new tag value, and click **OK** in the displayed dialog box.

**Figure 8-5** Editing a tag



scp-test-org

Policy Details

Name scp-test-org

URN organizations::e74e043fab784a45ad88f5ef6a4

Policy Type Service Control Policies

Description da

Edit Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Key Labs002

Value 002

Tags you can still add to this Policies: 19.

| Key | Value | Operation |
|---|---|---|
| Labs002 | 002 | Edit Delete |

**----End**

# 8.4 Viewing Tag Details

## 8.4.1 Viewing Tag Details for the Root, OUs, or Accounts

### Scenario

The following describes how to view tag details for the root, OUs, or accounts.

### Procedure

You view tag details for the root, OUs, and accounts in the same way. The following uses viewing tag details of an OU as an example.

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the OU whose tag details you want to view, and click the **Tags** tab in the pane on the right. The list of tags is displayed.

**Step 3** View all tags attached to the OU in the tag list.

**----End**

## 8.4.2 Viewing Tag Details for a Policy

### Scenario

The following describes how to view tag details for custom SCPs and tag policies.

### Procedure

The procedures for viewing tag details for SCPs and tag policies are similar. The following uses how to view tag details for custom SCPs as an example.

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

**Step 2** On the **Policies** page, click **Service control policies**.

**Step 3** Click the name of a policy to go to the policy details page.

**Step 4** Click the **Tags** tab to view all the tags attached to the SCP.

**----End**

# 8.5 Deleting a Tag

## 8.5.1 Deleting a Tag from the Root, OUs, or Accounts

### Scenario

The following describes how to delete a tag from the root, OUs, or accounts.

### Procedure

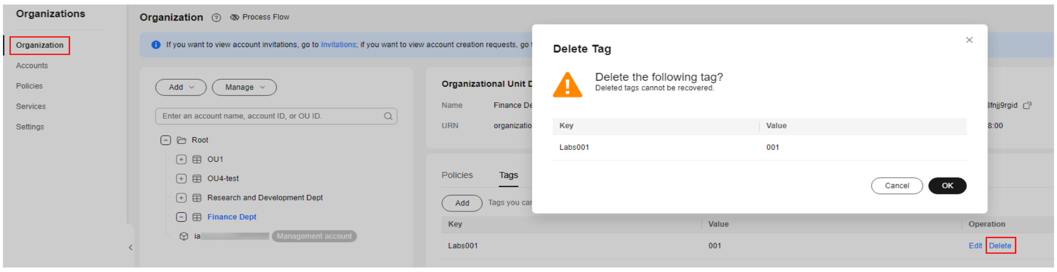
You delete tags from the root, OUs, and accounts in the same way. The following uses deleting a tag from an OU as an example.

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

**Step 2** Select the OU whose tag you want to delete, and click the **Tags** tab in the pane on the right.

**Step 3** Locate the tag you want to delete and click **Delete** in the **Operation** column. Then, click **OK** in the displayed dialog box.

**Figure 8-6** Deleting a tag



If you want to view account invitations, go to Invitations; if you want to view account creation requests, go t

Delete Tag

Delete the following tag?
Deleted tags cannot be recovered.

| Key | Value |
|---|---|
| Labs001 | 001 |

| Key | Value | Operation |
|---|---|---|
| Labs001 | 001 | Edit Delete |

**----End**

## 8.5.2 Deleting a Tag from a Policy

### Scenario

The following describes how to delete a tag from custom SCPs and tag policies.

### Procedure

The procedures for deleting tags from SCPs and tag policies are similar. The following uses how to delete tags from custom SCPs as an example.

**Step 1** Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

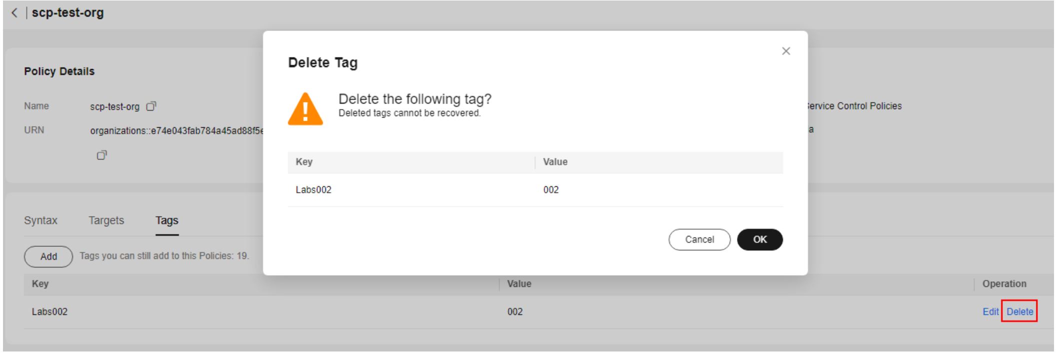
**Step 2** On the **Policies** page, click **Service control policies**.

**Step 3** Click the name of a policy to go to the policy details page.

**Step 4** On the **Tags** page, locate the tag you want to delete and click **Delete** in the **Operation** column.

**Step 5** Click **OK** in the displayed dialog box.

**Figure 8-7** Deleting a tag



Tags you can still add to this Policies: 19.

| Key | Value | Operation |
|---|---|---|
| Labs002 | 002 | Edit Delete |

Delete Tag

Delete the following tag?
Deleted tags cannot be recovered.

| Key | Value |
|---|---|
| Labs002 | 002 |

**----End**

# 9 CTS Auditing

## 9.1 Supported Organizations Operations

With Cloud Trace Service (CTS), you can record Organizations operations for later query, auditing, and backtracking.

**Table 9-1** Organizations operations that can be recorded by CTS

| Operation | Resource Type | Event Name |
|---|---|---|
| Creating an organization | Organization | createOrganization |
| Deleting an organization | Organization | celeteOrganization |
| Leaving an organization | Organization | leaveOrganization |
| Creating an OU | OrganizationUnit | createOrganizationalUnit |
| Updating an OU | OrganizationUnit | updateOrganizationalUnit |
| Deleting an OU | OrganizationUnit | deleteOrganizationalUnit |
| Inviting an account | Account | inviteAccount |
| Creating an account | Account | createAccount |
| Closing an account | Account | closeAccount |
| Updating an account | Account | updateAccount |
| Moving an account | Account | moveAccount |
| Removing an account | Account | removeAccount |
| Accepting an invitation | Handshake | acceptHandshake |
| Declining an invitation | Handshake | declineHandshake |
| Canceling an invitation | Handshake | cancelHandshake |

| Operation | Resource Type | Event Name |
|---|---|---|
| Enabling a trusted service | TrustedService | enableTrustedService |
| Disabling a trusted service | TrustedService | disableTrustedService |
| Configuring a delegated administrator | DelegatedAdministrator | registerDelegatedAdministrator |
| Removing a delegated administrator | DelegatedAdministrator | deregisterDelegatedAdministrator |
| Creating a policy | Policy | createPolicy |
| Updating a policy | Policy | updatePolicy |
| Deleting a policy | Policy | deletePolicy |
| Enabling a policy type | Policy | enablePolicyType |
| Disabling a policy type | Policy | disablePolicyType |
| Attaching a policy | Policy | attachPolicy |
| Detaching a policy | Policy | detachPolicy |
| Adding a tag | • Account<br>• OrganizationUnit<br>• Policy<br>• Root<br>• Tag | tagResource |
| Deleting a tag | • Account<br>• OrganizationUnit<br>• Policy<br>• Root<br>• Tag | untagResource |

# 9.2 Viewing CTS Traces in the Trace List

## Scenarios

After you enable Cloud Trace Service (CTS) and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, CTS starts recording operations on data in Object Storage Service (OBS) buckets. CTS stores operation records (traces) generated in the last seven days.

This section describes how to query or export operation records of the last seven days on the CTS console.

- Viewing Real-Time Traces in the Trace List of the New Edition
- Viewing Real-Time Traces in the Trace List of the Old Edition

## Constraints

- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces 5 minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.
- These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

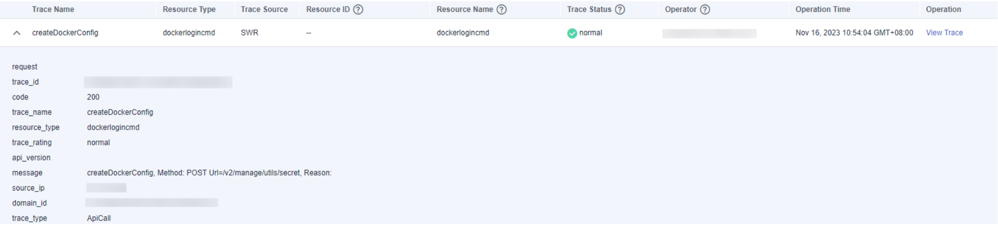
## Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.
   - **Operator**: Select one or more operators from the drop-down list.
   - **Trace Status**: Select **normal**, **warning**, or **incident**.
     - **normal**: The operation succeeded.
     - **warning**: The operation failed.
     - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.

   - Enter any keyword in the search box and press **Enter** to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
   - Click ↻ to view the latest information about traces.
   - Click ⚙ to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (●), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

## Viewing Real-Time Traces in the Trace List of the Old Edition

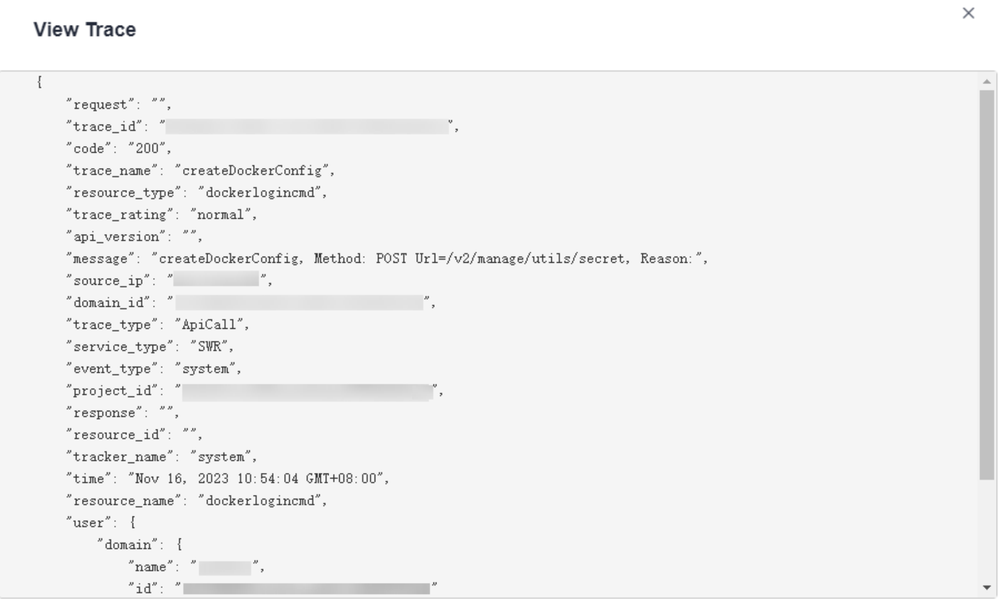
1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available.
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
   - Click ↻ to view the latest information about traces.
8. Click ⌄ on the left of a trace to expand its details.



| Trace Name | Resource Type | Trace Source | Resource ID ⓘ | Resource Name ⓘ | Trace Status ⓘ | Operator ⓘ | Operation Time | Operation |
|---|---|---|---|---|---|---|---|---|
| createDockerConfig | dockerlogincmd | SWR | -- | dockerlogincmd | ✓ normal | [redacted] | Nov 16, 2023 10:54:04 GMT+08:00 | View Trace |

| | |
|---|---|
| request | |
| trace_id | [redacted] |
| code | 200 |
| trace_name | createDockerConfig |
| resource_type | dockerlogincmd |
| trace_rating | normal |
| api_version | |
| message | createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason: |
| source_ip | [redacted] |
| domain_id | [redacted] |
| trace_type | ApiCall |

9. Click **View Trace** in the **Operation** column. The trace details are displayed.



View Trace

```
{
    "request": "",
    "trace_id": "[redacted]",
    "code": "200",
    "trace_name": "createDockerConfig",
    "resource_type": "dockerlogincmd",
    "trace_rating": "normal",
    "api_version": "",
    "message": "createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:",
    "source_ip": "[redacted]",
    "domain_id": "[redacted]",
    "trace_type": "ApiCall",
    "service_type": "SWR",
    "event_type": "system",
    "project_id": "[redacted]",
    "response": "",
    "resource_id": "",
    "tracker_name": "system",
    "time": "Nov 16, 2023 10:54:04 GMT+08:00",
    "resource_name": "dockerlogincmd",
    "user": {
        "domain": {
            "name": "[redacted]",
            "id": "[redacted]"
```

10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.

11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

# 10 Adjusting Quotas

## What Is Quota?

A quota is a limit on the quantity or capacity of a certain type of service resources that a user can use, for example, the maximum number of OUs you can create or the number of member accounts you can invite to an organization.

If a quota cannot meet your needs, apply for a higher quota.

## How Do I View My Quotas?

1. Log in to the management console.
2. Choose **Resources** > **My Quotas** in the upper right corner of the page.

   The **Service Quota** page is displayed.
3. View the used and total quotas of each type of resources on the displayed page.

   If a quota cannot meet your service requirements, apply for a higher quota.

## How Do I Increase My Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Service Quota** page is displayed.
3. Click **Increase Quota**.
4. On the **Create Service Ticket** page, set the parameters.

   In the **Problem Description** area, enter the required quota and the reason for the quota adjustment.
5. Read the agreements and confirm that you agree to them, and then click **Submit**.