

Tencent Cloud Organization

Operation Guide

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Operation Guide

Console Overview

Organization Settings

- Usage Limitations Description

- Creating Organization

- Viewing Organization Information

- Deleting Organization

- Viewing Invitation Information

- Accepting or Rejecting Invitation

- Quitting Organization

Department Management

- Creating Department

- Modifying Department Information

- Deleting Department

- Moving Member

Member Account Management

- Viewing Member List and Basic Information

- Removing Organization Member

- Adding Organization Member

- Canceling Member Invitation

- Creating Member Login Permission

- Configuring Member Login Permission

- Authorizing Sub-Users to Log in to Member Accounts

- Configuring Message Subscription for Created Member

Member Finance Management

- Organization Finance Overview

- Finance Management Mode

- Unified Organization Payment Mode (Pay-on-Behalf)

 - Pay-on-Behalf Mode Access Requirements

 - Supported Capabilities and Rules

- Member Self-Pay Mode

Member Access Management

- Service Control Policy

 - Overview

 - Enabling Service Control Policy

- Creating Custom Service Control Policy
- Viewing Service Control Policy Details
- Modifying Custom Service Control Policy
- Deleting Custom Service Control Policy
- Binding Custom Service Control Policy
- Unbinding Custom Service Control Policy
- Disabling Service Control Policy

Resource Management

- Organization Service Management
 - Overview
 - Managing Delegated Admin Account

Member Audit

- Auditing Member Log

Identity Center Management

- Introduction to Identity Center
 - Introduction to Identity Center
 - Basic Concepts
- Activate Services
- Manage Users
- Manage User Groups
- Settings
 - Manage SSO
- Manage Permission Configuration
 - Overview of Permission Configuration
 - Permission Configuration
 - Redeploy Permission Configuration
 - Undeploy Permission Configuration
- Manage Multi-account Authorization
 - Overview of Multi-Account Authorization
 - Configure CAM Role Synchronization
 - View/Modify/Delete Authorization
- Manage CAM User Synchronization
 - Configure CAM User Synchronization
 - View/Modify/Delete User Synchronization
- Identity Center User Login

Operation Guide

Console Overview

Last updated : 2024-03-06 18:40:46

The TCO console offers the account management features. The organization creator can create organizational structures, invite or add members to organizations, set finance management policies for members, and share resources to members. The specified features are as listed below:

| Name | Feature |
|---------------------------|--|
| Organization settings | Creating an organization |
| | Viewing the organization information |
| | Deleting an organization |
| | Viewing the invitation information |
| | Accepting or rejecting an invitation |
| | Leaving an organization |
| Department management | Creating a department |
| | Modifying the department information |
| | Deleting a department |
| | Moving a member |
| Member account management | Viewing the member list and basic member information |
| | Removing a member |
| | Inviting a member |
| | Canceling a member invitation |
| | Granting a member the account access |
| Service control policy | Service control policy overview |
| | Enabling a service control policy |
| | Creating a custom service control policy |
| | |

| | |
|--------------|---|
| | Viewing service control policy details |
| | Modifying a custom service control policy |
| | Deleting a custom service control policy |
| | Binding a custom service control policy |
| | Unbinding a custom service control policy |
| | Disabling a service control policy |
| Member audit | Auditing member logs |

Organization Settings

Usage Limitations Description

Last updated : 2024-03-06 18:40:46

I. Scenario and Restriction Descriptions

| Functional Module | Account Management Operation Scenario | Distributor Sub-Customer | Direct Sales Customer |
|--------------------|---------------------------------------|---|--|
| Account management | Creating a member account | The newly created member account is bound to the same distributor sub-customer relationship as the management account by default and inherits the enterprise identity verification entity of the admin account by default. | The identity verification entity of the newly created member account should either match the that of the admin account or be another already associated entity. |
| | Inviting a member account | The account to be invited must be the same distributor sub-customer, and the identity verification entity of the enterprise must match that of the admin account. Moreover, it should not be part of any other organization or have pending invitations from other organization accounts. | The account to be invited must be a direct sale customer, and the identity verification entity should match that of the admin account or be another entity that is already associated. Moreover, it should not be part of any other organization or have pending invitations from other organization accounts. |
| | Quitting the organization account | Member departure from the organization is not supported. | Member departure from the organization is not supported. |
| Finance management | Viewing financial overview | Admin accounts can view the summary of paid bills on behalf of organization members. | Not Supported. |
| | Pay-on-behalf | The consumption of member accounts is uniformly paid by the admin account. | The consumption of member accounts is uniformly paid by the admin account. |
| | | | |

| | | | |
|--|--------------------|---|---|
| | Self-pay | Not Supported. | Members are responsible for their own consumption (Created members must select pay-on-behalf at first. They can switch to self-pay after accounts are opened with bound cards). |
| | Viewing bills | The admin account has the capacity to view the detailed bills of its members. | The admin account has the capacity to view the detailed bills of its members. |
| | Viewing balance | Not Supported. | The admin account can access the balance details of its corresponding member accounts. |
| | Inheriting offers | Not Supported. | Member accounts can inherit the discounts of the admin account. |
| | Consolidated bills | Not Supported. | The admin account consolidates the charges of multiple member accounts for download. |
| | Issuing invoices | Not Supported. | The admin account has the ability to issue invoices on behalf of member accounts. |

II. System Limit Descriptions

| Module | Limitation | Limit Value |
|--------------|--|-------------|
| Member | Number of members to be created (the number of identity verification accounts) | 5 |
| Department | Number of departments level | 5 |
| | Number of sub-departments to be created | 20 |
| Member Login | Custom login permissions | 20 |
| | Custom login permissions associated with preset policy | 30 |
| | Custom login permissions associated with custom policy | 1 |

Creating Organization

Last updated : 2024-03-06 18:40:46

If you complete enterprise identity verification and haven't joined or created an organization, you can create one in the TCO console.

Directions

Log in to the TCO console, click [basic information](#) on the left sidebar, and click **Create** to create an organization.

Note:

Only users that complete enterprise identity verification can create an organization. For more information, see [enterprise identity verification guide](#).

After creating the organization successfully, you cannot join another organization until the created organization is deleted.

Only direct customers and distributor sub-customers of Tencent Cloud are allowed to use the group account, and the account types within the group organization must be consistent.

Viewing Organization Information

Last updated : 2024-03-06 18:40:46

The organization admin or members can view the department information in the organization in the TCO console.

Directions

Log in to the TCO console and select **Department management** on the left sidebar to view the organization information, including department names and IDs, member names and IDs, permission scope, and payment mode.

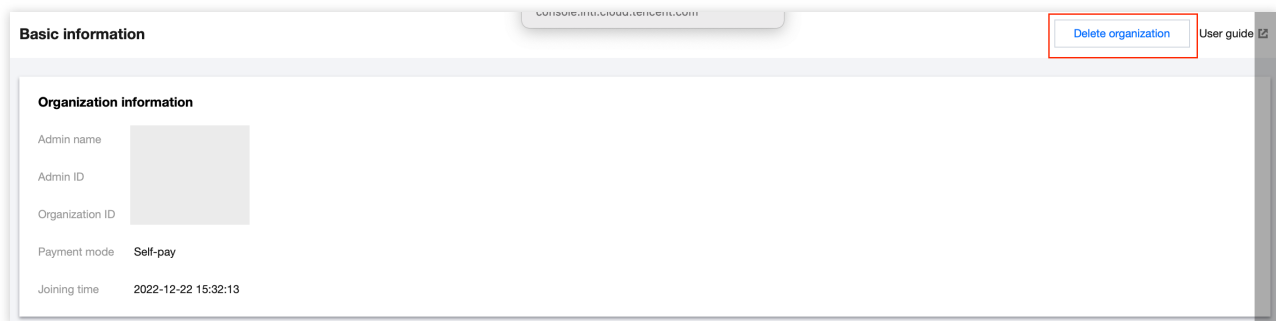
Deleting Organization

Last updated : 2024-03-06 18:40:46

The organization creator can delete the created organization.

Directions

1. Log in to the TCO console and click **Organization settings** > **Basic information** on the left sidebar.
2. On the **Basic information** page, click **Delete organization** in the top-left corner.



3. In the **Delete organization** pop-up window, click **OK**.

In the following cases, the organization cannot be deleted directly:

There is still a member account in the organization.

The organization is sharing a resource.

Viewing Invitation Information

Last updated : 2024-03-06 18:40:46

You can view the information of invitations from organizations in the TCO console.

Directions

Log in to the TCO console and click [Basic information](#) on the left sidebar to view records.

Note:

You can view the invitation information if you haven't joined any organization.

The invitation list only displays the invitation records within the last three months.

Each invitation record is valid for up to 15 days.

Accepting or Rejecting Invitation

Last updated : 2024-03-06 18:40:46

You can accept or reject invitations from organizations in the TCO console.

Directions

Log in to the TCO console and click **Basic information** on the left sidebar. On the **Basic information** page, you can view valid invitation records and click **OK** to join an organization.

To refuse to join the organization, click **Reject**.

Note:

Only users that completed enterprise identity verification can join an organization. For more information, see [Enterprise Identity Verification Guide](#).

Your verified entity must be the same as the invitee or has been added to the organization's verified entity information.

After you join the organization, the invitation list will be hidden until you quit the organization.

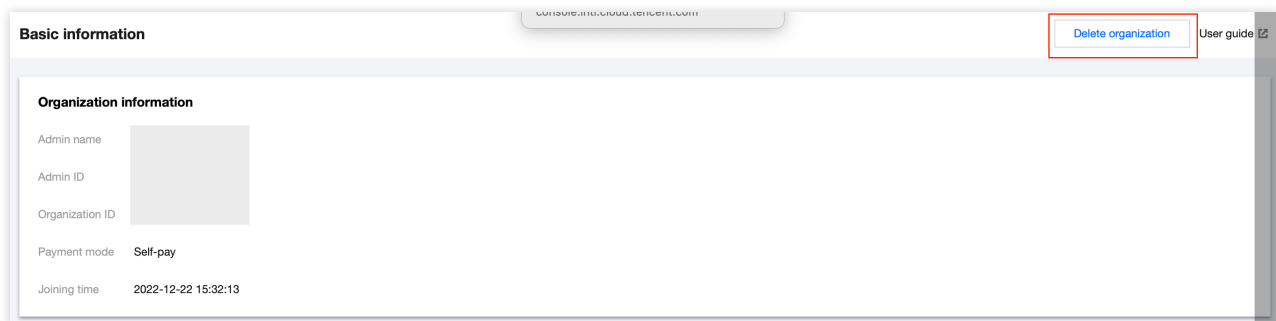
Quitting Organization

Last updated : 2024-03-06 18:40:46

An organization member can quit an organization in the TCO console.

Directions

1. Log in to the TCO console and click **Basic information** on the left sidebar.
2. On the **Basic information** page, click **Delete organization**.



3. In the **Delete organization** pop-up window, click **OK**.

In the following cases, you cannot directly quit the organization:

The organization admin forbids you from quitting the organization.

Your account is created within the organization.

Department Management

Creating Department

Last updated : 2024-03-06 18:43:08

This document describes how to create a department in the TCO console. The organization creator can manage members by department.

Note:

An organization can contain up to five levels of department relationships.

Directions

1. Log in to the TCO console and select **Department management** on the left sidebar.
2. On the **Department management** page, click **Add department**.

The screenshot displays the 'Add department' interface in the Tencent Cloud Organization console. It features a search bar for department names and a dropdown menu for selecting a root unit. The sidebar on the right provides additional context for the selected unit, including basic information and a member list.

3. In the **Add department** pop-up window, select a root unit name, enter the department name and description, and select tags.
4. Click **OK**.

Modifying Department Information

Last updated : 2024-03-06 18:43:08

This document describes how to modify the department information in the TCO console.

Directions

Log in to the TCO console, select **Department management** on the left sidebar, and modify the department information as needed.

Renaming a department

Click



on the right of the department name. In the pop-up **Edit department name** window, enter a new name and click **OK**.

Edit department name

Department name

Root

The department name can contain up to 40 characters.

OK

Cancel

Modifying the department description or tag

In the window on the right of the **Organizational structure** page, click



on the right of the description or tag. In the pop-up window, edit the content and click **OK**.

Add departmentDelete department

Please enter the department name

Root(Root)

Root(Root)

Basic information

Department nameRoot(Root)

Department ID

Description

Tag

Member list

Add member

| <input type="checkbox"/> | Name |
|--------------------------|---------|
| <input type="checkbox"/> | test_02 |
| <input type="checkbox"/> | test_01 |

Please enter descriptions

OKCancel

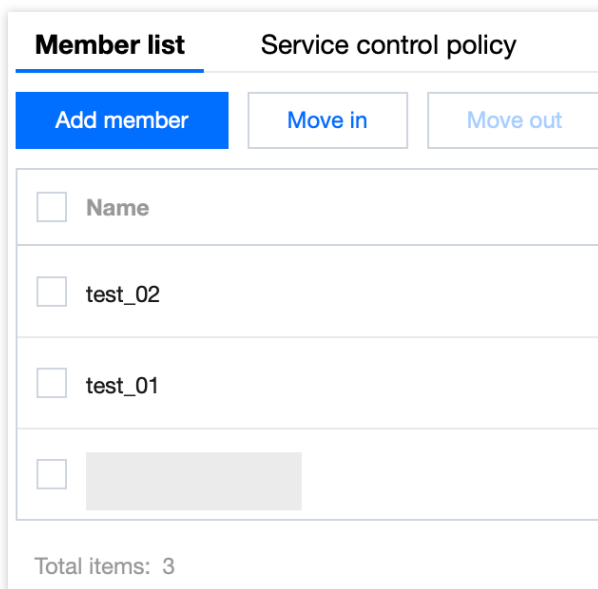
Deleting Department

Last updated : 2024-03-06 18:43:08

You can delete an organization in the TCO console when you no longer need it.

Directions

1. Log in to the TCO console and select **Organization structure** on the left sidebar.
2. On the **Organization structure** page, select the target department and click **Delete department** above.



3. In the **Delete department** pop-up window, click **Delete**.

Moving Member

Last updated : 2024-03-06 18:43:08

A new member is placed under the root unit directory by default. The organization creator can move the member to the target department.

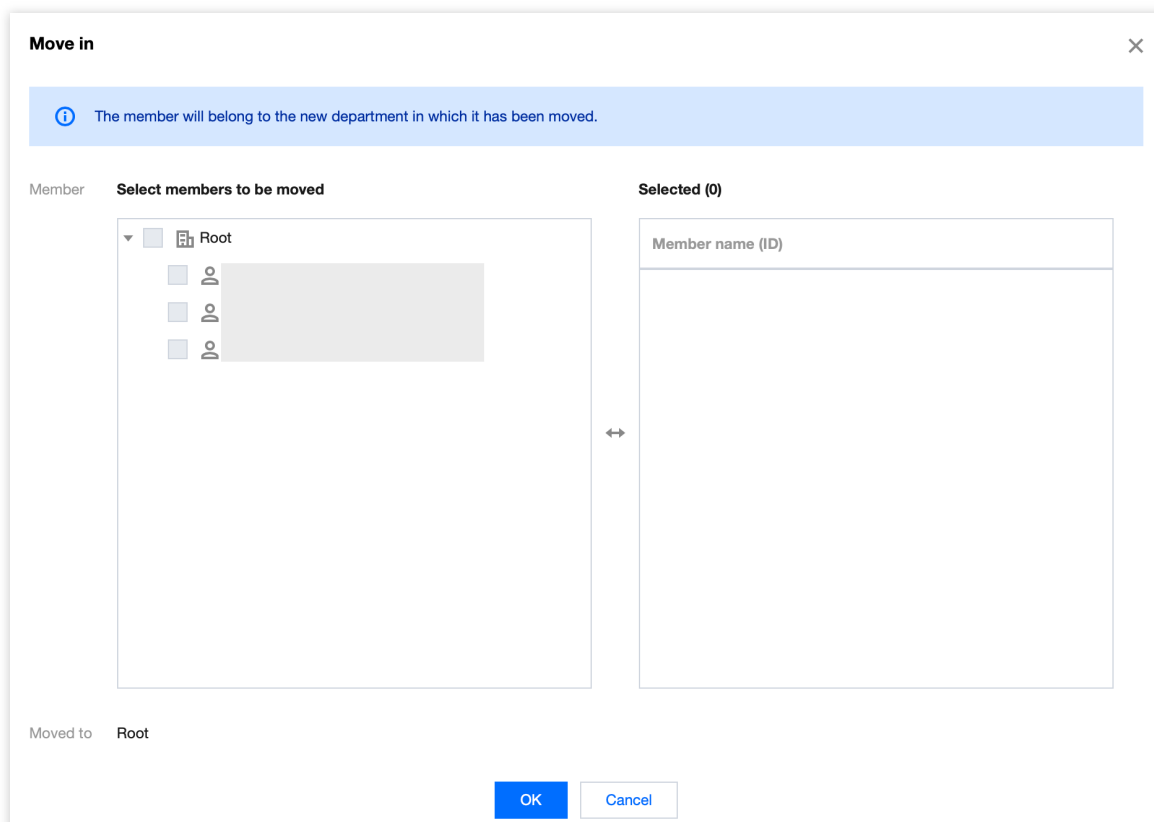
Directions

1. Log in to the TCO console and select **Department management** on the left sidebar.
2. In the window on the right of the **Organization structure** page, perform the following operations as needed:

Adding a member

Moving a member

1. Select **Move in** in **Member list** on the right.
2. In the **Move in** pop-up window, select the target member and click **OK**.



1. Select **Move out** in **Member list** on the right.
2. In the **Move out** pop-up window, select the target department and click OK.

Move member

Target department

Root

OK

Cancel

Member Account Management

Viewing Member List and Basic Information

Last updated : 2024-03-06 18:43:09

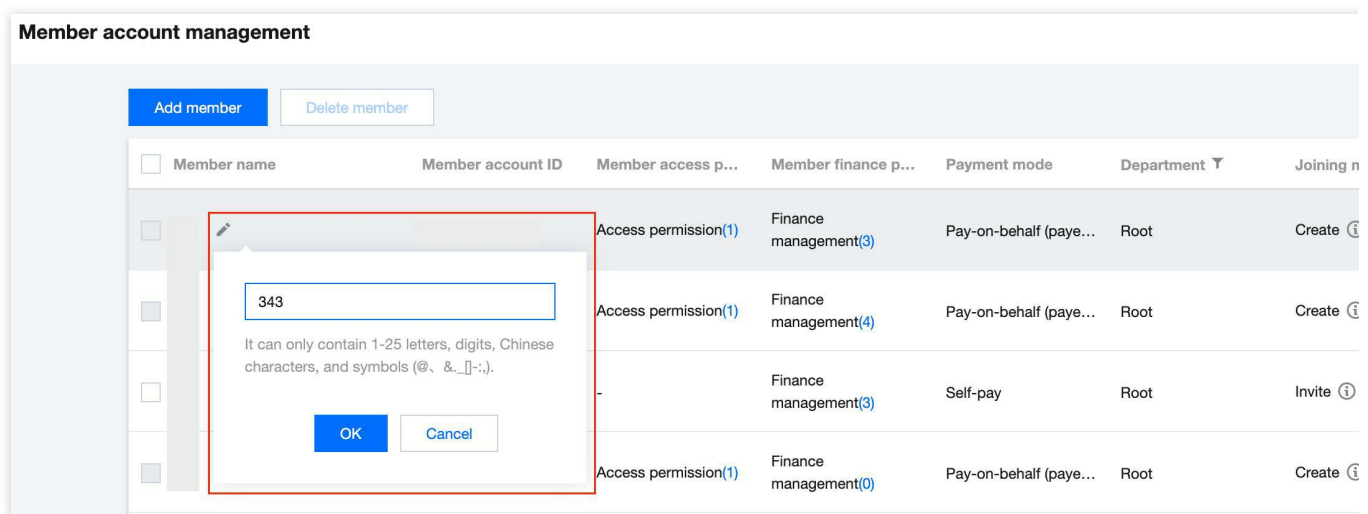
This document describes how to view the member list and basic member information in the TCO console.

Directions

1. Log in to the TCO console and select **Member account management** on the left sidebar to view the information of members in the current organization.


The member information includes the member name, member account ID, access permission, finance permission, payment mode, department, joining method, and whether the member is allowed to quit the organization. You can change the member name, finance permission, payment mode, and department.

2. To modify a member name, go to the **Member list** page and click the edit icon next to the member name you want to modify. In the pop-up editing box, enter the new member name and click **OK** to save your modification.



3. To modify a member's department, click **Edit** on the right of the target member in the **Operation** column. In the **Edit member** pop-up window, select the target department in the **Department** drop-down list and click **OK** to save your modification.

Edit member ✕

 For a created member, the finance authorization change will take effect immediately.

Member name * 343

Finance permission * ☒ Finance management

☒ View bills ☒ View balance ☒ Aggregate payments
☐ Invoice

Payment mode Self-pay **Pay-on-behalf**

Payer

Before you pay on behalf of other accounts, make sure your account balance is sufficient. For details, see [here](#).


Department Root

Active quitting supported ☐ Created members cannot actively quit the organization.

OK Cancel

4. To modify a member's finance permission or payment mode, click **Edit** on the right of the target member in the **Operation** column. In the **Edit member** pop-up window, modify the finance permission and payment mode as needed, and click **OK** to save your modification.

Edit member✕

 For a created member, the finance authorization change will take effect immediately.

Member name *

343

Finance permission *

☒ Finance management

☒ View bills

☒ View balance

☒ Aggregate payments

☐ Invoice

Payment mode

Self-pay

Pay-on-behalf

Payer

Before you pay on behalf of other accounts, make sure your account balance is sufficient. For details, see [here](#).

Department

Root

Active quitting supported

☐

Created members cannot actively quit the organization.

OK

Cancel

Removing Organization Member

Last updated : 2024-03-06 18:43:08

This document describes how to remove an organization member in the TCO console.

Note:

A removed member cannot be viewed or edited in the member list and cannot be displayed or moved in the organizational structure.

The organization creator account cannot be removed.

Directions

1. Log in to the TCO console and click **Member account management** on the left sidebar.
2. You can remove one or multiple members:

Remove one member: Click **Remove** on the right of the target member and click **OK** in the pop-up window.

Batch remove members: Select the target members and click **Delete member** above the member list.

Adding Organization Member

Last updated : 2024-07-09 17:01:46

The organization creator can add a member to an organization through invitation or creation.

Directions

Choose a method of adding a member as needed:

Inviting a member

Creating a member

I. Direct Client Scenario:

1.
Log in to the
TCO console and click [member account management](#) on the left sidebar.
2. On the member account management page, click **Add member**.
3. On the **Add member** page, select **Invite member**.

4. Set the account ID, member name, finance permission, payment mode, department, and whether to allow the member to actively quit the organization. You can obtain the account ID on the [account information](#) page.
5. Click **OK**, and the information of the invited member will be verified. The account you invite must have completed enterprise identity verification and cannot have joined any other organization before. The verified entity of the invited account needs to be either the same as or associated with that of the admin account. If the association is not completed, contact your sales rep.
6. After the member is successfully invited, the invitation information will be retained for 15 days. You can check the invitation records by selecting [organization change record](#) on the left sidebar and selecting the **Member invitation record** tab.

Page 27 of 131

II. Distributor Sub-Customer Scenario

Note:

In a distribution scenario:

It is necessary to ensure that the distribution relationship of all the member accounts in the group are unified, i.e., member accounts and admin accounts must belong to the same distributor. When a new account is invited to join the organization, the prerequisites must be met that the invited account and the group administrator belong to the same distributors.

The payment mode for a member account only supports pay-on-half currently.

1. Log in to the Tencent Cloud Organization console and select [member account management](#) on the left sidebar.
2. On the member account management page, click **Add member**.
3. On the **Add member** page, select **Invite member**.
4. Fill in account ID, member name, department, and whether to allow the member to actively quit the organization.

The account ID can be obtained on the [account information](#) page.

Note:

View bills is chosen for finance permission by default in the distributor sub-customer scenario. The payment mode temporarily only supports pay-on-behalf.

If it is necessary to create a department, you can refer to [add department](#).

5. Upon completion, click **Confirm**. The information verification of the invited member is required. The verification content is as follows:

The invited account needs to complete the enterprise real name authentication and doesn't join any group or organization.

The enterprise real name authentication entity must align with the management account.

It is essential to ensure the unified distribution relationship for all the member accounts under the group, i.e., the member account and the administration account belong to the same distributor.

6. Once the invitation is successful, the invitation information will remain valid for 15 days. You can choose [organization change record](#) on the left sidebar, and choose the **Member invitation record** tab to view the invitation details, as shown below:

Organization change record

Member change record

Department change record

Member invitation record

Member creation record

Member department change record

Finance authorization change record

Member name

Account ID

Status ▾

Payment mode

Department name (ID)

I. Direct Client Scenario:

Note:

The organization

creator can create members under the current entity (which is the admin account's entity) or other entities.

Creating a member under the current entity

1. Log in to the TCO console and click [member account management](#) on the left sidebar.
2. On the member account management page, click **Add member**.

After a member account is successfully created, it will use the entity of the admin account for identity verification. An admin role (OrganizationAccessControlRole) will be added for the created account and granted to the ad

Adding method

Create member
Create a Tencent Cloud root account and add it to the organization

Invite member
Invite a Tencent Cloud root account that is in use to join the organization

Member name *

Please enter the name

The name must be unique in the organization and can contain 1-25 letters, digits, Chinese characters, or symbols (@, & _ [] ~:).

Entity ⓘ

Current entityOther entities

Name of the current verified entity: [REDACTED]

Member finance authorization

☒ View bills

☒ View balance

☒ Consolidate bills

☐ Invoice

☐ Inherit offer

☐ Cost Analysis

☐ Budget management

Payment mode

Self-payPay-on-behalf

Payer

[REDACTED]

Before you pay on behalf of other accounts, make sure your account balance is sufficient. For details, see [here](#).

Department

Root

Create department

After a member account is successfully created, it will use the selected entity for identity verification. An admin role will be created for the member account and granted to the admin account. You can create and configure login permission on the [Login permission settings](#) and [Multi-member authorization management](#) pages respectively. For more information, see [Documentation](#).

OK

Cancel

3. Fill in the fields according to your needs: **Member name**, **Entity**, **Finance permission**, and **Department**.

For the entity, select **Current entity**.

To create members, select **Pay-on-behalf** by default.

You can create a department as instructed in [creating department](#).

4. Click **OK**, and the member account will be created automatically and inherit the identity information of the creator.

You can select [organization change record](#) on the left sidebar and click **Member change record** > **Member**

creation record to view the creation record and result.

Organization change record

Member change record Department change record

Member invitation record **Member creation record** Member department change record Finance authorization change record

Please

| Member name | Account name | Member account ID | Status ▾ | Member access p... | Payment mode | Department name ... | Description | Applic |
|-------------|--------------|-------------------|----------|--------------------|--------------|---------------------|-------------|--------|
|-------------|--------------|-------------------|----------|--------------------|--------------|---------------------|-------------|--------|

Creating a member under other entities

1. Contact your sales rep to apply to associate with other entities.
2. After the entity is successfully associated, log in to the [TCO console](#) and select **Verified entity management** on the left sidebar. In the entity list, click **Invite member** in the **Operation** column to invite the member under the target entity to join the organization. For details, see the **Inviting a member** tab in [this document](#).

Verified entity management

Entity list Entity adding record

ⓘ The organization admin account can apply to add the information of other verified entities of the organization. After that, the admin account can invite an account under the added entities to join its organization under the corresponding entity.

Create entity

Please

| Entity name | Entity type | Adding Date | Accounts under entity | Entity admin account |
|-------------|-------------|---------------------|-----------------------|-----------------------|
| | Admin | | | |
| | Member | 2023-03-03 17:20:03 | 0 | - Set |

Total items: 2

10 ▾ / page

3. Return to the [verified entity management](#) page and click **Edit entity admin account** to set the entity admin.

Set entity admin account

After setting the entity admin account, you can use the entity to create a member, and the created member account will use the entity for enterprise identity verification. The information of the created account can only take effect after the admin account's confirmation.

Entity name *

Admin account name (ID) *

Please select ▼

OK

Close

4. Under the **Entity list** tab on the **Verified entity management** page, click **Create member** to enter the **Add member** page and select **Create member** as the adding method.

5. Complete all the other required information, select **Other entities** as the entity, and select an entity in the drop-down list.

Note:

Self-pay is selected by default when a member is created.

If it is necessary to create a department, you can refer to [add department](#).

6. The entity admin account will review the member creation application, and the member can be successfully created after the application is approved. The created member account will inherit the enterprise identity information of the entity admin account. You can select [organization change record](#) on the left sidebar and click **Member change record** > **Member creation record** to view the creation record and result.

Organization change record

Member change record

Department change record

Member invitation record

Member creation record

Member department change record

Finance authorization change record

Please

| Member name | Account name | Member account ID | Status ▾ | Member access p... | Payment mode | Department name ... | Description | Applic |
|-------------|--------------|-------------------|----------|--------------------|--------------|---------------------|-------------|--------|
|-------------|--------------|-------------------|----------|--------------------|--------------|---------------------|-------------|--------|

II. Scenario: Sub-Customer Reseller

1. Log in to the Tencent Cloud Organization console and choose [member account management](#) on the left sidebar.

2. On the member account management page, click **Add Member**.

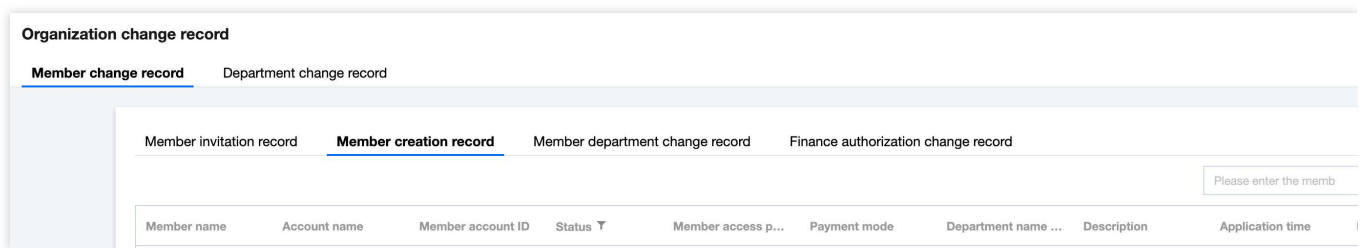
3. Enter the name and department as required.

Note:

View bills is chosen for finance permission by default in the distributor sub-customer scenario. The payment mode temporarily only supports pay-on-behalf.

If it is necessary to create a department, you can refer to [add department](#).

4. Upon clicking **OK**, a member account will be created automatically, which will inherit the enterprise real name information of the creator. You can choose **Member Change Record > New Member Record** to view the creation record and its results in [organization change record](#) on the left sidebar, which is shown below:



5. The created member inherits the enterprise real name verification entity of the admin account by default and binds the same distributor sub-account relationship as the admin account.

Canceling Member Invitation

Last updated : 2024-03-06 18:43:09

The organization creator can cancel an invitation before the invitee accepts it.

Directions

1. Log in to the TCO console and select **Organization change record** on the left sidebar.
2. On the **Organization change record** page, select **Member change record** > **Member invitation record**, and click **Cancel invitation** on the right of the target invitee.
3. In the pop-up window, click **OK**.

Creating Member Login Permission

Last updated : 2024-03-06 18:43:08

Overview

TCO allows the organization admin to **create login permissions** for members to manage member permissions in a refined manner. Authorized sub-users can only log in to the member account within the permission scope. This document describes how to create a member login permission in the TCO console.

Directions

Creating Login Permission

1. Log in to the TCO console and select [Login permission settings](#) on the left sidebar.
2. Click **Create login permission**.
3. In the pop-up window, configure the permission name and select permission policies as needed. The details are as shown below:

Note:

For more information about policies, see [Basic Concepts](#).

Create login permission ✕

Permission name *

Permissions policy * **Select associated policies (835 in total)** ?

Support search policy name

Policy name

☐ AdministratorAccess

☐ QCloudResourceFullAccess

☐ ReadOnlyAccess

☐ QCloudFinanceFullAccess

☐ QcloudAAFulAccess

☐ QcloudABFullAccess

Selected (0)

Policy name

↔

You can select multiple items by holding down the Shift key.

Description

OK

Close

4. Click **OK**.

Note:

Admin is the default permission, with which a member account can have the admin permission. The organization admin can create up to 20 custom permissions.

Configuring Member Login Permission

Last updated : 2024-03-06 18:43:09

Overview

This document describes how to configure or delete a created member login permission in the TCO console.

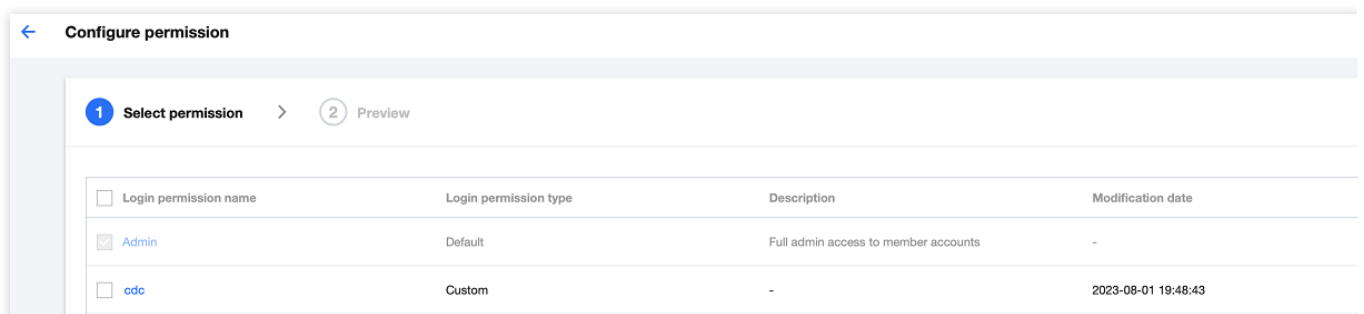
Directions

Configuring member login permission

1. Log in to the TCO console and select [Multi-member authorization management](#) on the left sidebar.
2. In the member list, select the members for which you want to configure login permissions.
3. Click **Configure permission**.

3.1 Select permission

Select permissions in the permission list as needed. The details are as shown below:



| Configure permission | | | |
|--|-----------------------|--------------------------------------|---------------------|
| 1 Select permission > 2 Preview | | | |
| <input type="checkbox"/> Login permission name | Login permission type | Description | Modification date |
| <input checked="" type="checkbox"/> Admin | Default | Full admin access to member accounts | - |
| <input type="checkbox"/> cdc | Custom | - | 2023-08-01 19:48:43 |

3.2 Preview and confirm

On the preview page, confirm the member account and permission information.

← Configure permission

✓ Select permission > 2 Preview

Selected member account

| Member name | Member account ID |
|-------------|-------------------|
| user | 100031975199 |

Selected login permission

| Login permission name | Login permission type | Description | Modification date |
|-----------------------|-----------------------|--------------------------------------|---------------------|
| Admin | Default | Full admin access to member accounts | - |
| cdc | Custom | - | 2023-08-01 19:48:43 |

Complete Previous

4. Click **Complete**.

Note:

You can select up to 10 members at a time.

The permission list contains all the default and custom login permissions.

You cannot configure login permissions for members invited before the login permission configuration feature was released. To do so, contact the sales rep.

Deleting member login permission

Option 1:

1. Log in to the TCO console and select [Multi-member authorization management](#) on the left sidebar.
2. Select the target member and click **Delete permission** in the **Operation** column.
3. In the pop-up window, select the permission to be deleted.
4. Click OK.

Option 2 :

1. Log in to the TCO console and select [Multi-member authorization management](#) on the left sidebar.
2. Select a member and click the member name to enter the member details page.
3. On the **Member details** page, select the permission you want to delete and click **Delete** in the **Operation** column.

← Member details

Basic information

Member name user Member account ID

Existing permission

Configure permission

| Login permission name | Login permission type | Description | Modification date | Operation |
|-----------------------|-----------------------|--------------------------------------|---------------------|-------------|
| Admin | Default | Full admin access to member accounts | 2023-06-14 19:24:51 | Edit Delete |
| cdc | Custom | - | 2023-08-01 19:48:58 | Delete |
| tag_admin | Custom | - | 2023-06-14 19:29:14 | Delete |

Total items: 3

10 / page

4. In the pop-up window, click **OK**.

Authorizing Sub-Users to Log in to Member Accounts

Last updated : 2024-03-06 18:43:08

Overview

The organization admin can authorize sub-users to log in to and manage member accounts by creating organization management policies. This document describes how to do so in the console.

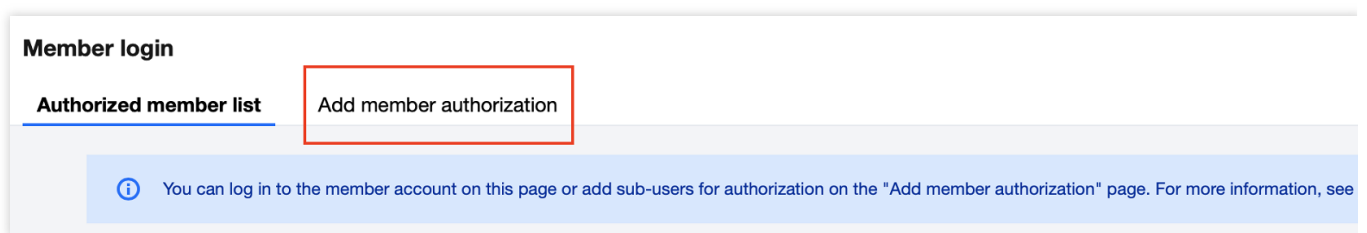
Note:

If the member account is newly created, please wait for 15 minutes before logging in, otherwise, you may not be able to enter the Tencent Cloud Console normally.

Directions

1、Adding authorization

1. Log in to the TCO console and select [Member login](#) on the left sidebar.
2. Select the **Add member authorization** and click **Add authorization**. The details are as shown below:



3. In the pop-up window, select members and permissions and enter the authorization policy name. The details are as shown below:

←

Add member authorization

1 Create authorization policy

>

2 Select sub-user for authorization

Select member

Select member accounts (79 in total) You can select up to 10 members for policy association at a time.

Search by member name/ID

| Member name | Account ID |
|---|------------|
| <input checked="" type="checkbox"/> RDC | |

Selected (1)

| Member name | Account ID |
|-------------|------------|
| RDC | |

You can select multiple items by holding down the Shift key.

Select permission

Login permission

Admin

[View login permission](#)

If you select multiple members, the drop-down list will display the intersection of their login permissions.

Enter the policy name

Authorization policy name

test

It can contain up to 128 letters, digits, and symbols (+, =, ., @, _ -).

Next

Cancel

Note:

The policy created in this step is an organization management policy.

Member selection: You cannot authorize members invited before the sub-user authorization feature was released. To do so, contact the sales rep.

Permission selection: When you select multiple members, the permission list will display the intersection of the login permissions of the selected members.

Authorization policy name: Enter a custom policy name.

4. Click **Next** and select the sub-accounts you want to authorize. The details are as shown below:

← Add member authorization

✓ Create authorization policy > 2 Select sub-user for authorization

Select sub-user

Select the sub-accounts to be associated (58 in total) Up to five sub-accounts can be associated at a time.

You can enter keywords (separated by space or tab key) to search for sub-account name/ID

| Account name | ID |
|---------------------------------|----|
| <input type="checkbox"/> abc001 | |

Selected (0)

| Account name | ID |
|--------------|----|
|--------------|----|

You can select multiple items by holding down the Shift key.

Complete Previous

5. Click **Complete** to complete the authorization.

2、Logging in to the console with the sub-account

After completing the authorization, you can log in to the console with the sub-account to perform management operations.

1. Log in to the TCO console with the authorized sub-account and select [Member login](#) on the left sidebar.
2. On the member login page, select the member account to which you want to log in and click **Log in** in the **Operation** column. In the pop-up window, select a login permission. The details are as shown below:

Log in to member account

ⓘ You can only select one permission for login at a time.

Login permission * Please select

|

Admin

Note:

You can select one permission at a time.

You can only log in to the member account as an authorized sub-user.

3、 Canceling authorization

1. Log in to the TCO console and select [Member login](#) on the left sidebar.
2. On the **Add member authorization** page, click **Unbind** in the **Operation** column.
3. Click **OK** to cancel the authorization.

Note:

If you cancel the authorization, this operation will also apply to all other members who have authorized this policy.

4、 Managing sub-users' permission to log in to member accounts

The root account of the organization admin can view the list of all member accounts to which the sub-user can log in and can revoke the sub-user's login permission.

1. Log in to the TCO console and select [Member login](#) on the left sidebar.
2. On the **Authorized member list** page, select the target member and click **Revoke permission** in the **Operation** column.
3. On the **Add member authorization** page, select the permission to be revoked and click **Unbind** in the **Operation** column.
4. Click **OK**.

Configuring Message Subscription for Created Member

Last updated : 2024-03-06 18:43:09

Overview

By default, members created in the TCO console do not have contact information and therefore cannot receive notification messages via SMS or email. This document describes how to configure message subscription for created members.

Directions

1. Log in to the TCO console as instructed in [Granting Member Account Access](#).
2. Log in to the CAM console and select **Users** > [User List](#) on the left sidebar.
3. On the **User List** page, click a username to enter the user details page.
4. Click the

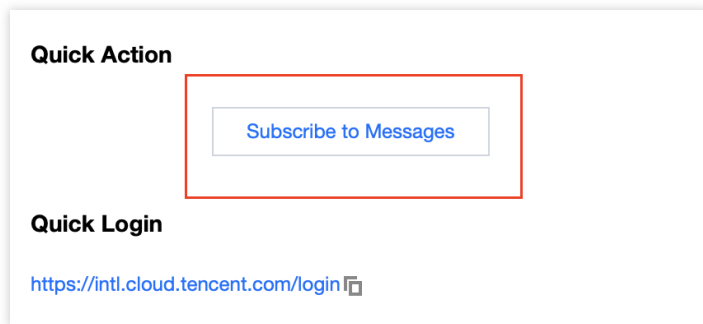


icon next to each contact method and add the mobile number and email for the member as prompted.

Root Account Root Account Edit Info

| | | | | |
|------------|---|------------------|---|---------------------------|
| Account ID | | Contact Number ⓘ | - | Replacing |
| Remarks | - | Contact Email ⓘ | - | Replacing |

5. After that, click **Subscribe to Messages** in the **Quick Action** module on the right.



6. In the pop-up window, select the message types as needed.

Note:

You can also create a sub-user under the member account and receive messages via the sub-user as instructed above.

Member Finance Management

Organization Finance Overview

Last updated : 2024-03-06 18:45:06

The group financial overview allows admin accounts to view and manage the corporate consumption by dimensions such as members and products. Corporate admin accounts can uniformly view and manage the consumption of all accounts within the company, thus enhancing the efficiency of financial management.

Note:

1. The group financial overview is currently only available to distributor sub-customers and only displays cost trends and bill details for pay-on-behalf.
2. The group financial overview regularly synchronizes the current month's bill data every morning. If a member joins the group after the 1st of the month, the financial data for that month is not be visible for the member (except for the admin account).
3. The group bill overview does not display cost trends and bill details prior to the creation of the group organization.
4. The organization account only allows admin accounts to view the financial overview within the organization. For a complete view of bill details, please go to [billing](#).

The steps are as follows:

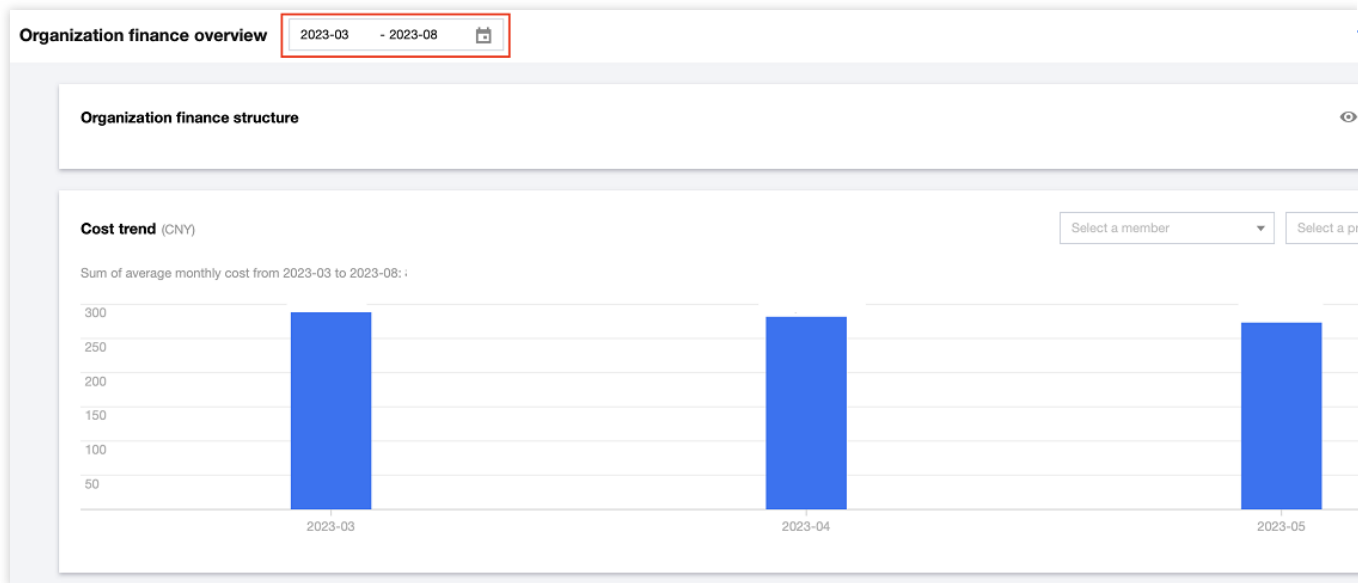
Viewing cost trends and bill details

1. Log in to the [Tencent Cloud Organization console](#), then select **Group Finance Overview** from the left-hand navigation.
2. On the **Group Financial Overview** page, select the appropriate time at the top. Select a member and a product in the **Cost trend** module. The corresponding cost trends and bill details will be displayed.

Note:

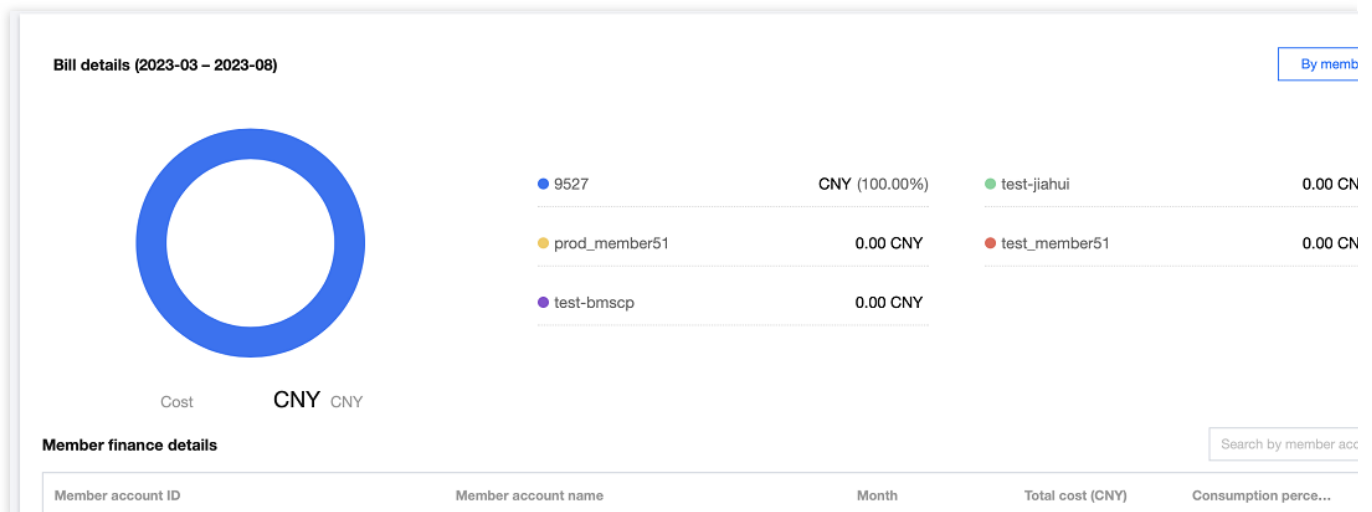
Once you enter the **Group Financial Overview** page, it will display the financial overview details for the recent half year of all the members and products by default.

The maximum time interval for cost information is six months. Details with the time interval exceeding this value are not supported for display.



3. In the **Cost trend** module, you can view the cost trend chart and the specific consumption amounts each month and the average total monthly cost for the selected product of the selected member within the selected time.

4. In the **Bill details** module, you can view the cost details of the selected member for the selected product within the selected time. In the top right corner, you can choose to display **By member** or **By product** according to your needs.



(1) If By member is selected:

A pie chart displaying the Top 5 member accounts by total consumption amount is shown above, with the specific member account names, corresponding amounts, and proportions displayed on the right.

A financial list of the selected members is displayed below, including **member account ID**, **Member account name**, **Month**, **Total cost (CNY)**, **Consumption percentage**, and **Operation**. Clicking **Operation** will display the product consumption distribution diagram for a member during the selected period.

(2) If By product is selected:

A pie chart displaying the Top 5 products by total consumption amount is shown above, with the specific product names, corresponding amounts, and proportions displayed on the right.

A financial list of the selected products is displayed below, including **Product name**, **Month**, **Total cost**, **Consumption percentage**, and **Operation**. Clicking **Operation** will display the member consumption distribution diagram for a product during the selected period.

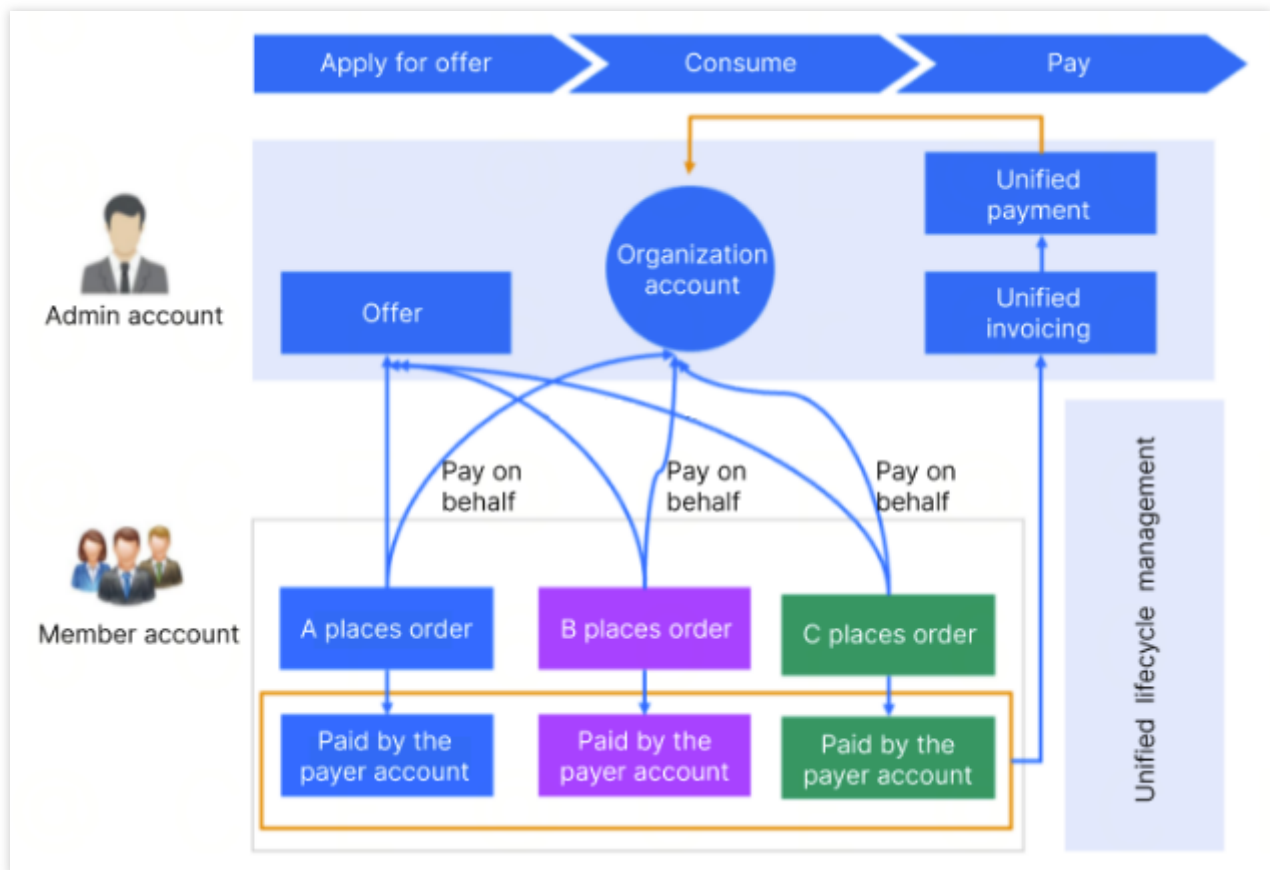
Finance Management Mode

Last updated : 2024-03-06 18:45:06

TCO integrates the finance management methods of organization users to provide the **unified organization payment mode** and **member self-pay mode**. You can select a suitable finance management mode as needed.

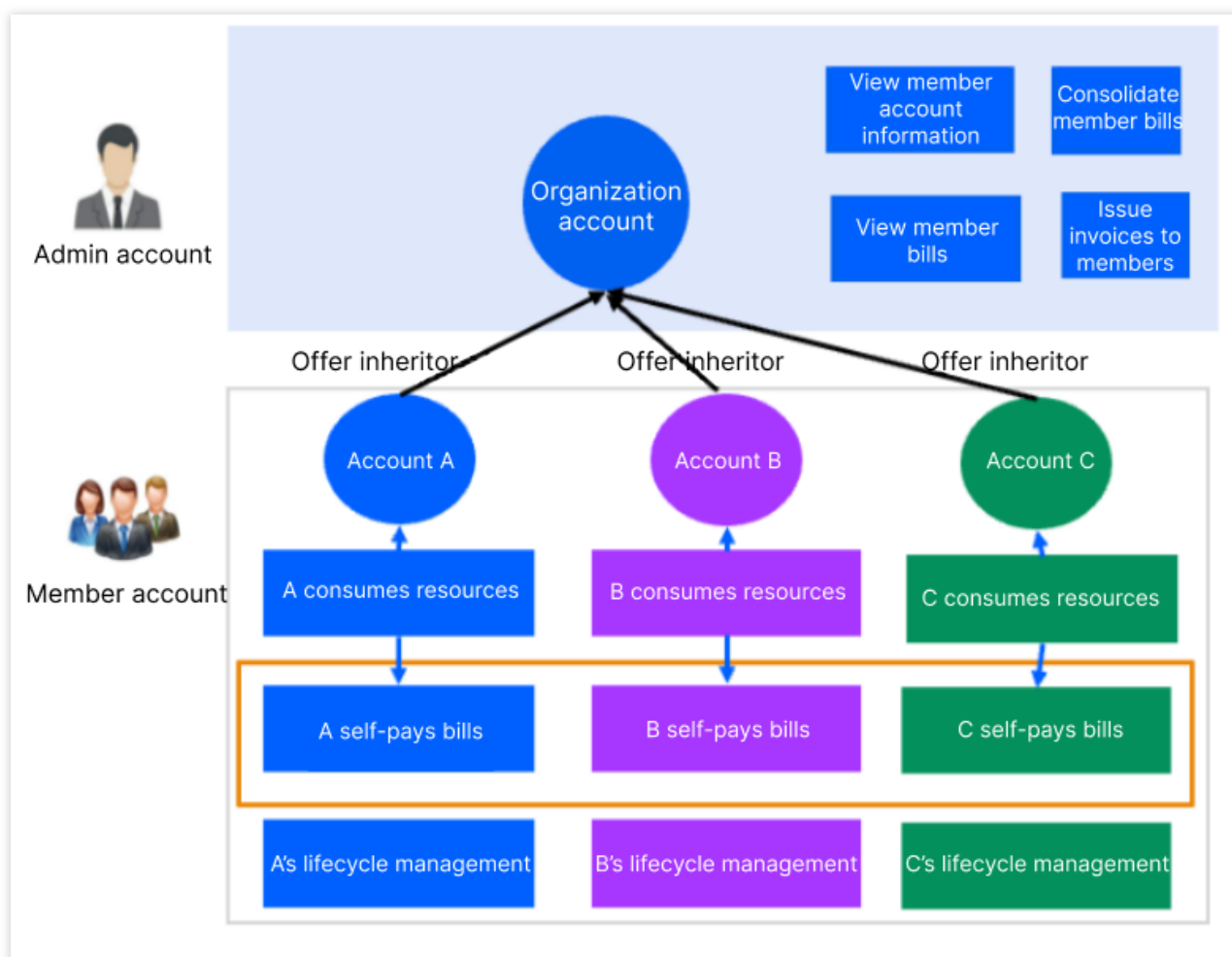
Unified Organization Payment Mode

In unified organization payment mode, member accounts top up the admin account, and the consumption of each member account is automatically paid by the admin account uniformly, with no need of fund allocation. For users of the same entity, the admin can be set as the payer account to automatically pay for their used resources.



Member Self-Pay Mode

In this mode, the organization admin account can view the account and bill information of its members, issue invoices to members, and consolidate members' bills. If member accounts and the admin account are under the same verified entity, the former can inherit the latter's offers specified in the contract. Besides, member accounts pay for the resources they consume by themselves.



Unified Organization Payment Mode (Pay-on-Behalf)

Pay-on-Behalf Mode Access Requirements

Last updated : 2024-03-06 18:45:06

Pay-on-Behalf Access Requirements

Requirements for enabling pay-on-behalf mode: When a member account joins an organization, the account must meet the following requirements to enable the pay-on-behalf mode:

| Object | Condition |
|----------------|---|
| Member account | Account verification: 1. Member and admin accounts must be verified with the same enterprise identity at Tencent Cloud. 2. Agents and their customers cannot select the financial pay-on-behalf mode. 3. Distributor sub-customers only support the pay-on-behalf mode. Under the distribution mode, additional verification is required: 1. Verify whether administrators and members belong to the same distributor. 2. Verify whether the sub-customer account possesses any sub-customer vouchers. If such vouchers exist, they must first be fully utilized or invalid. |
| | Account type verification: 1. External accounts or internal accounts of type 4, 6, or 9: The available balance in the member account should be greater than or equal to 0. 2. Internal accounts of other types: Not verified. |
| | Order verification: The member account cannot have orders to be paid, renewed, or refunded. Order status: To be paid or processing. |
| Admin account | Currently, only the admin account can be the payer account, while agents, resellers, and their customers cannot. 1. External accounts or internal accounts of type 4, 6, or 9: The payer account has no overdue payments or has an available balance greater than or equal to 0 . 2. Internal accounts of other types: Not verified. |

Requirements for disabling pay-on-behalf mode: When a member account quits an organization, the account must meet the following requirements to disable the pay-on-behalf mode:

| | |
|--|--|
| | |
|--|--|

| Object | Condition |
|----------------|---|
| Member account | Account type verification: 1. External accounts or internal accounts of type 4, 6, or 9: The available balance in the member account should be greater than or equal to 0. 2. Internal accounts of other types: Not verified. |
| | Order verification: The member account cannot have orders to be paid, renewed, or refunded\\. Order status: To be paid or processing. |
| | Card verification: Mid- and long-tail member accounts not followed up by channel managers should have a bound credit card. |

Supported Capabilities and Rules

Last updated : 2024-03-06 18:45:06

The unified organization payment mode is a financial pay-on-behalf mode including the following capabilities:

| Capability | Description |
|---------------------|--|
| Orders | Member accounts' monthly subscription and pay-as-you-go orders are automatically paid by the payer account. |
| Offers | This capability is optional. If member accounts have the offer inheritance permission, the offer inheritance rules will apply; otherwise, member accounts will use their own offers. |
| Vouchers | Member accounts use the admin account's vouchers by default. |
| Bills | Member accounts' bills are automatically settled to the payer account for unified management. |
| Invoices | Member accounts' invoiceable amounts are automatically settled to the payer account for unified invoice issuance. |
| Transaction details | Member accounts' transaction details are uniformly managed by the payer account. |
| Lifecycle | Overdue payments, service suspension, and top-up under member accounts are processed based on the balance of the payer account. |

Relevant rules are as detailed below:

Orders

Purchasing/upgrading monthly subscribed resource

When a member account purchases/upgrades a monthly subscribed resource, only payment-on-behalf can be selected, and payment with balance or online payment are not supported. Then, the payer account doesn't need to process the order manually, and the system will automatically complete the payment-on-behalf based on the balance and credit of the payer account and display the pay-on-behalf result.

Please confirm the following product information

Order 20221228477001275208691

sp_ckafka_profession

440.00 USD

Region: Guangzhou

Unit Price: 440.00USD/month

AZ: Shanghai Zone 3

Instance Name: Not named

Specs Type: Pro Edition

Kafka Version: 1.1.1

Peak Bandwidth: 40MB/s

Disk capacity: 500GB

Topic: 400

Partition: 800

Message Retention Period: 24 hours

Network: vpc-moja8o5

Subnet: subnet-9hgdvumy

Check the Fe

sp_ckafka_profess

ayment:

Deduction

Please Select a Payment Method

Order Amount: 440.00 USD



Request for pay-on-behalf

Pay: 440.00 USD

Your organization has enabled pay-on-behalf mode for your account. If you need to invoice the order, please contact the payer account.

Confirm pay-on-behalf

Vouchers and discounts

Your organization has enabled pay-on-behalf mode for your account. Vouchers under your own account will not be used. [了解详情](#)





Payment succeeded

Your order has been paid successfully

Here's a help article for your reference: [Invoicing Guide](#)

[View My Orders](#)[Go to Console](#)

Downgrading/unsubscribing monthly subscribed resource

When a member account downgrades or unsubscribes from a monthly subscribed resource, the amount will be refunded to the payer account based on the UIN and payment ratio.

You can learn about the rules by referring to the following scenario:

Below are the member account details:



| Order | Pay-on-Behalf | Account to Refund to |
|---|--|---|
| The order is placed in region A and refunded in region B. | No | The amount is refunded to the member account based on the payer UIN. |
| | Yes (the resource may be upgraded in region B) | The amount is refunded to the member and admin accounts based on the payer UIN. |

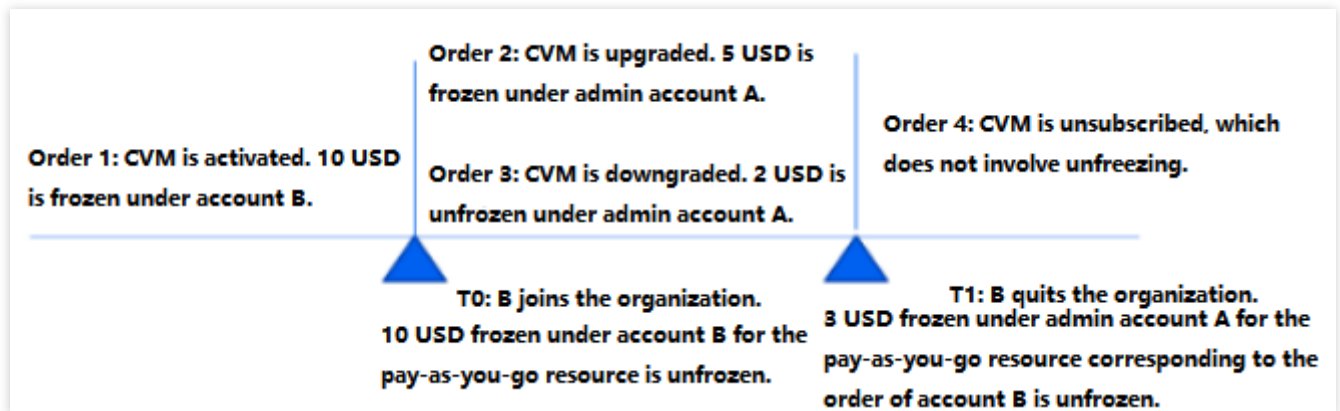
| | | |
|---|--|---|
| The order is placed in region B. | Yes | The amount is refunded to the admin account based on the payer UIN. |
| The order is placed in region A and refunded in region C. | No | The amount is refunded to the member account based on the payer UIN. |
| | Yes (the resource may be upgraded in region B) | The amount is refunded to the member and admin accounts based on the payer UIN. |

Amount freezing upon pay-as-you-go resource activation

When a member account joins an organization, the frozen amount of the member account's pay-as-you-go resources will be unfrozen.

When the member account quits the organization, the member account's order corresponding to the admin account's frozen amount of pay-as-you-go resources will be unfrozen.

Below is an example:



Pay-as-you-go resource settlement

The fees incurred within the current or next cycle will be deducted from the payer account.

The fees incurred within the last cycle will be deducted from the member account.

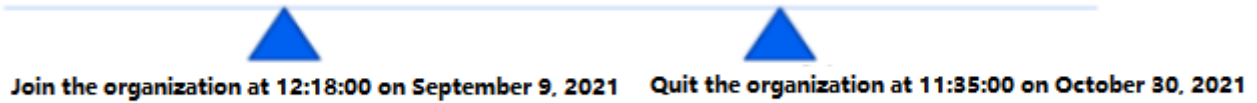
Note:

The rules also apply to the extended cycle of pay-as-you-go resources.

Vouchers: Member accounts can use the payer account's vouchers.

Resource pack: The rules for product purchase, upgrade/downgrade, unsubscription are the same as those for monthly subscribed products. Currently, fees incurred by pay-as-you-go resources cannot be paid on behalf; instead, they will be deducted from the member account's own resource pack.

Below is an example:



| Settlement Cycle | Example | Settlement Rule | Resource Pack Deduction |
|------------------|---------------------------------|--|--|
| Hourly | 2021-09-09 12:00:00–13:00:00 | The fees and vouchers are deducted from the payer account. | The fees are deducted from the member account's own resource pack. |
| | 2021-10-30 11:00:00–12:00:00 | The fees are deducted from the member account, and vouchers can be used. | The fees are deducted from the member account's own resource pack. |
| Daily | 2021-09-09 | The fees and vouchers are deducted from the payer account. | The fees are deducted from the member account's own resource pack. |
| | 2021-10-30 | The fees are deducted from the member account, and vouchers can be used. | The fees are deducted from the member account's own resource pack. |
| Monthly | 2021-09 | The fees and vouchers are deducted from the payer account. | The fees are deducted from the member account's own resource pack. |
| | 2021-10 | The fees are deducted from the member account, and vouchers can be used. | The fees are deducted from the member account's own resource pack. |

Viewing pay-on-behalf orders

After a payment-on-behalf is completed, you can log in to the [TCO console](#) and select **Pay-on-behalf order management** on the left sidebar to view the pay-on-behalf order and perform relevant operations based on your role.

Admin account

The admin account can view the pay-on-behalf orders of member accounts. For orders to be paid, the admin account can also pay on behalf or cancel them.

Tencent Cloud Organization

- Member Management
- Organizational Structure
- Organizational Settings
- Pay-on-behalf Order Management**

Order Management

Prepaid Order | Postpaid Order

This page only shows orders you pay on behalf of others. To view your own orders, go to [Order Management](#)

[Consolidated Payment](#) | [Cancel](#) | 2022-10-03 ~ 2023-01-03

Order no./instance ID

| <input type="checkbox"/> | Member account ID | Member name | Order No. | Product | Subproduct |
|--------------------------|-------------------|-------------------|-------------------------|---------------------|--------------------------|
| <input type="checkbox"/> | 200029082654 | 200029082654-intl | 20221229654000042185521 | cloud block storage | Premium cloud block stor |
| <input type="checkbox"/> | 200029082654 | 200029082654-intl | 20221229654000042223221 | cloud block storage | Premium cloud block stor |
| <input type="checkbox"/> | 200029082654 | 200029082654-intl | 20221229654000042185161 | cloud block storage | Premium cloud block stor |

Total items: 3

Member account

A member account can view all orders paid by the payer account and apply for payment-on-behalf on the page.

Tencent Cloud Organization

Member Management

Organizational Structure

Organizational Settings

Pay-on-behalf Order Management

Pay-on-behalf Bill Management

Order Management

Prepaid Order

Postpaid Order

Consolidated Payment

Cancel

2022-10-03 ~ 2023-01-03

Order no./instance ID

| Member account ID | Member name | Order No. | Product | Subproduct |
|-------------------|------------------|-------------------------|---------------------|-------------------------|
| 200029082654 | 242753776@qq.com | 20221229654000042185521 | cloud block storage | Premium cloud block sto |
| 200029082654 | 242753776@qq.com | 20221229654000042223221 | cloud block storage | Premium cloud block sto |
| 200029082654 | 242753776@qq.com | 20221229654000042185161 | cloud block storage | Premium cloud block sto |

Total items: 3

Offers

In financial pay-on-behalf mode, the admin account can set whether to enable “offer inheritance” for member accounts. If it is enabled, the offer inheritance rules will apply; otherwise, member accounts will use their own offers.

Note:

Offers cannot be inherited for products in the blocklist, for which the member accounts' own offers will apply. For more information on the blocklist, contact your channel manager or submit a ticket for assistance.

Rebates of the payer account are not inherited by member accounts.

The admin account can set whether to enable “offer inheritance” for member accounts. If “offer inheritance” is enabled, the existing offer inheritance relationship will be verified. If a member chooses an admin account as its payer, they can't establish a new inheritance relationship if any of them is already an inheritor of other accounts.

If you want to cancel the existing offer inheritance relationship and establish a new one, contact your sales rep to confirm that the payer account has successfully applied for contract offers and to help cancel the existing offer inheritance relationship. If you have any questions, [submit a ticket](#).

Vouchers

Member accounts can use the admin account's vouchers but not their own vouchers.

Bills

Member accounts' bills are automatically settled to the payer account for unified management. The payer account can view the bills of all associated member accounts, and a member account can only view its own bills paid by the payer account but not the bills of other member accounts.

Paid-on-behalf bills can be viewed in the [TCO console](#), while self-paid bills can be viewed in the [Billing Center](#). For more information on the bill fields, see [Fields in Bills](#).

Below are the bills from the perspectives of the admin account and member account respectively:

Admin account

Member account

After logging in to the Tencent Cloud console, the admin account can go to [Billing Center -> Bills](#) to view pay-on-behalf bills.

Billing Center

Bill Details 2023-01

Bill by Instance Bill Details Consolidated Bill

The current month's final bill for resource consumption will be generated on the 3rd day of the upcoming month. Prior to this date, deductions are not final and are for reference purposes only. Expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. Actual deduction amount will be in 2 decimal places. For more information, see [Billing Center -> Bills](#).

All products Please choose one product All Projects All Regions All AZs All Billing Modes

All transaction types All Tags ☐ Do not display \$0 transactions

Total Cost (Including Tax) **1.12 USD** = Total Amount After Discount (Excluding Tax) **1.04 USD** - Voucher Deduction **0.00 USD** + Tax Amount **0.08 USD**

| Instance ID | Instance Name | Product Name | Payer Account ID | Owner Account... | Operator Account ID | Subproduct Name |
|-----------------------|---------------|----------------------------|------------------|------------------|---------------------|----------------------|
| ri-pabo2bqa | | Cloud Virtual Machine(CVM) | 100010445724 | 100010445724 | 200025986183 | CVM Standard S5 |
| ri-bu6fgu4q | | Cloud Virtual Machine(CVM) | 100010445724 | 100010445724 | 200025986183 | CVM Standard S5 |
| ri-8xt2argu | | Cloud Virtual Machine(CVM) | 100010445724 | 100010445724 | 200025986183 | CVM Standard S5 |
| 100010445724-std_s... | | Cloud Object Storage | 100010445724 | 100010445724 | 100010445724 | cos standard storage |

Total items: 4 20 / page

Billing Center

Bill Details 2023-01

Bill by Instance **Bill Details** Consolidated Bill

The current month's final bill for resource consumption will be generated on the 3rd day of the upcoming month. Prior to this date, deductions are not final and are for reference purposes only. Expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. Actual deduction amount will be in 2 decimal places. For more information, see [Billing Center -> Bills](#).

All products Please choose one product Please choose one subproduct All Projects All Regions All AZs All Billing Modes

All Billing Modes All transaction types ☐ Do not display \$0 transactions

Total Cost (Including Tax) **1.47 USD** = Total Amount After Discount (Excluding Tax) **1.36 USD** - Voucher Deduction **0.00 USD** + Tax Amount **0.10 USD**

| Instance ID | Instance Name | Product Name | Payer Account ID | Owner Account... | Operator Account ID | Billing Mode |
|-------------|---------------|----------------------------|------------------|------------------|---------------------|-------------------------|
| ri-8xt2argu | | Cloud Virtual Machine(CVM) | 100010445724 | 100010445724 | 200025986183 | Pay-As-You-Go resources |
| ri-8xt2argu | | Cloud Virtual Machine(CVM) | 100010445724 | 100010445724 | 200025986183 | Pay-As-You-Go resources |
| ri-8xt2argu | | Cloud Virtual Machine(CVM) | 100010445724 | 100010445724 | 200025986183 | Pay-As-You-Go resources |
| ri-8xt2argu | | Cloud Virtual Machine(CVM) | 100010445724 | 100010445724 | 200025986183 | Pay-As-You-Go resources |

Total items: 4 20 / page

After logging in to the Tencent Cloud console, the member account can go to [Tencent Cloud Organization -> Pay-on-behalf bill management](#) to view pay-on-behalf bills.

Tencent Cloud Organization

- Member Management
- Organizational Structure
- Organizational Settings
- Pay-on-behalf Bill Management
- Bill Overview
- Bill Details

Bill Details
2022-12
📅

Bill by Instance
Bill Details

ⓘ This page only shows orders you pay on behalf of others. To view your own orders, go to [Bills](#).
 The current month's final bill for resource consumption will be generated on the 3rd day of the upcoming month. Prior to this date, deductions are not final and are for ref
 Expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. Actual deduction amount will be i

All products

Please choose one product

All Projects

All Regions

All AZs

All transaction types

☐ Do not display \$0 transactions

Total Cost (Including Tax) **10.00 USD** = Total Amount After Discount (Excluding Tax) **10.00 USD** - Voucher Deduction **0.00 USD** + Tax Amount **0.00**

| Instance ID | Instance Name | Product Name | Subproduct Name | Billing Mode | Instance Type |
|---------------|---------------|--------------|-----------------|----------------------|---------------|
| 0147749369471 | | trade_t_s | =C47 | Monthly subscription | - |

◀

Total items: 1

Invoices

Member accounts are verified with the same enterprise identity as the payer account, and invoices are issued by the payer account uniformly.

Transaction details

Member accounts' transaction details are uniformly managed by the payer account.

Lifecycle

The payer account should guarantee a sufficient balance to ensure that the member accounts' resources can be used normally. For resources that need to be renewed manually, the payer account should renew them timely. Below are the rules for overdue payment, service suspension, and resource termination events:

Message events

Messages about monthly subscribed resources such as notifications for resource expiration/termination and service suspension/recovery will be sent to the payer account.

Messages about pay-as-you-go resources will be sent to the member account.

Action events

Service suspension and termination events under member accounts are processed based on the balance of the payer account. If the payer account has an overdue payment, the service will be suspended for all associated member accounts.

After the payer account is topped up to a positive balance, the service will be recovered for all associated member accounts.

Status processing

After a member account joins an organization, service suspension and recovery will be subject to the balance, credit, or privileges of the payer account.

After a member account quits an organization, service suspension and recovery will be subject to its own balance, credit, or privileges.

Miscellaneous

If you and Tencent Cloud have entered into a contract for private cloud businesses, the billing rules stipulated in the contract shall prevail.

Member Self-Pay Mode

Last updated : 2024-03-06 18:45:06

The member self-pay mode involves the following finance permissions:

| Finance Permission | Description |
|-----------------------------------|---|
| View member account information | The admin account can view the balance information of member accounts. |
| View member account bills | The admin account can view the bill details of member accounts. |
| Issue invoices to member accounts | The admin account can issue invoices to member accounts. |
| Consolidate bills | The admin account can consolidate the bills of multiple member accounts for download. |
| Inherit offers | Member accounts can inherit the admin account's offers specified in the contract. |

Viewing Member Account Balance

This section describes how the admin account views the balance information of its member accounts.

Directions

1. Log in to the **Billing Center** console with the admin account and select [Account Info](#) on the left sidebar.
2. In the drop-down list in the top-right corner, select a member account to view its balance information.

The screenshot shows the 'Billing Center' sidebar on the left with 'Account Info' selected. The main content area is titled 'Account Info' and contains a notice about credit limits, an 'Outstanding Amount' section showing 500.00 USD with a 'Pay Now' button and a 'Monthly Expense Alert' toggle, a 'Promo voucher' section showing 1 voucher, and an 'Available Credit' section showing 0.30 USD. A table at the bottom right lists account balances: Credit Limit (1.00 USD), Unsettled Amt. (0.00 USD), Outstanding Amount (500.00 USD), and Frozen Amount (0.70 USD).

Billing Center

- Account Info
- Order Management
- Renewal Management
- Payment Management
- Bills
- Cost Management
- Vouchers
- Download Records

Account Info

In order to provide you with a better experience, we will give you a certain credit limit, allowing you to spend within the credit limit for any Tencent Cloud services. We will automatically deduct the payment for each month based on your billing cycle. You can also make an early payment. Once the bill is paid successfully, your available credit will be restored.

Outstanding Amount

500.00 USD [Pay Now](#) Monthly Expense Alert ☒

| | | |
|------------|---|----------------|
| Due Amount | + | Amount Overdue |
| 0.00USD | | 500.00USD |

Promo voucher

1 voucher (1 voucher will expire in 7 days)

0.00USD

Available Credit

0.30 USD

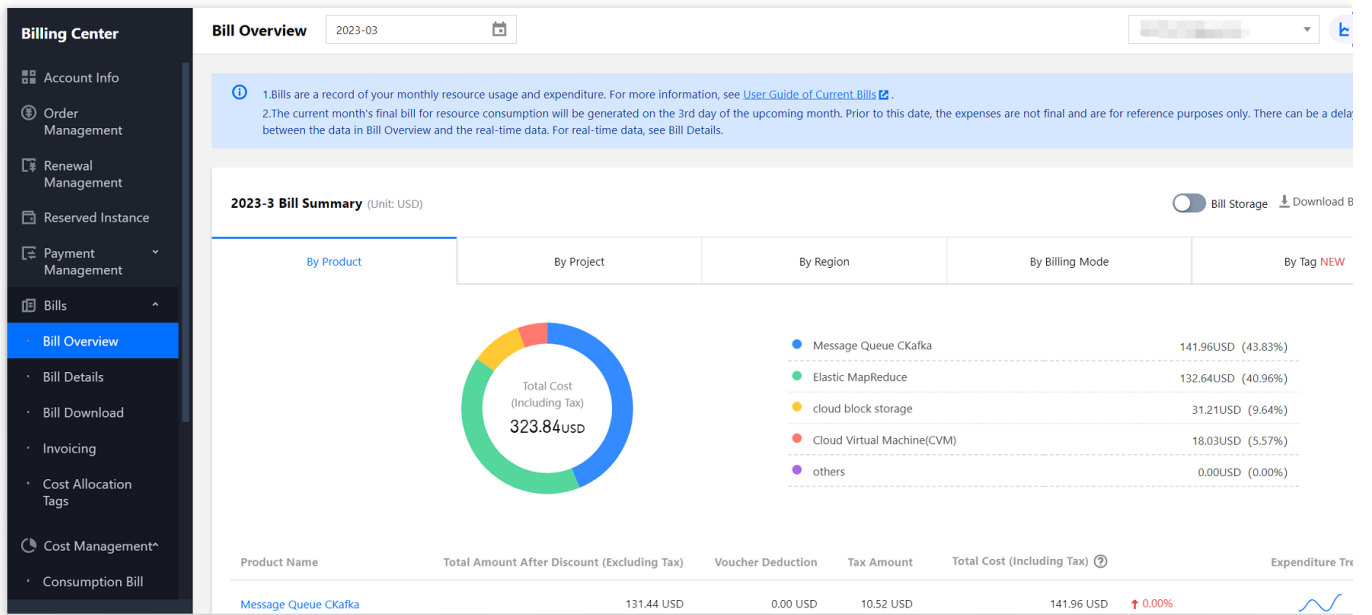
| | |
|--------------------|------------|
| Credit Limit | 1.00 USD |
| Unsettled Amt. | 0.00 USD |
| Outstanding Amount | 500.00 USD |
| Frozen Amount | 0.70 USD |

Viewing Member Account Bills

This section describes how the admin account views the bill details of member accounts.

Directions

1. Log in to the **Billing Center** console with the admin account and select **Bills** on the left sidebar.
2. On the **Bill Overview** page, select a member account in the drop-down list in the top-right corner to view its bill overview.
3. On the **Bill Details** page, select a member account in the drop-down list in the top-right corner to view its bill details. You can also click **Confirm Bill** to confirm the bill for the member account for the selected month.



Billing Center

- Account Info
- Order Management
- Renewal Management
- Reserved Instance
- Payment Management
- Bills
 - Bill Overview
 - Bill Details**
 - Bill Download
 - Invoicing
 - Cost Allocation Tags
- Cost Management
- Consumption Bill

Bill Details 2023-03 Confirm Bill

Bill by Instance Bill Details Consolidated Bill

① The current month's final bill for resource consumption will be generated on the 3rd day of the upcoming month. Prior to this date, deductions are not final and are for reference purposes only. Expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. Actual deduction amount will be in 2 decimal places. For more details, see [User Guide of Current Bills](#).

All products Please choose one product All Projects All Regions All AZs All Billing Modes

All transaction types All Tags ☐ Do not display \$0 transactions

Total Cost (Including Tax) **323.84 USD** = Total Amount After Discount (Excluding Tax) **299.85 USD** - Voucher Deduction **0.00 USD** + Tax Amount **23.99 USD**

| Instance ID | Instance Name | Product Name | Payer Account ID | Owner Account... | Operator Account ID | Subproduct Name | Billing Mode |
|-----------------|---------------|----------------------|------------------|------------------|---------------------|-------------------|----------------------|
| ckafka-kz25boea | Not named | Message Queue CKafka | | | | ckafka-profession | Monthly subscription |
| emr-vm-pjb7eq2t | EMR-ywpwj4xg | Elastic MapReduce | | | | emr-sa2 | Pay-As-You-Go resou |
| emr-vm-l1fwioz | EMR-ywpwj4xg | Elastic MapReduce | | | | emr-sa2 | Pay-As-You-Go resou |
| emr-vm-26iomzfv | EMR-ywpwj4xg | Elastic MapReduce | | | | emr-sa2 | Pay-As-You-Go resou |
| emr-vm-pjb7eq2t | EMR-ywpwj4xg | Elastic MapReduce | | | | emr-sa2 | Pay-As-You-Go resou |

Billing Center

Bill Details 2023-02

Bill by Instance | **Bill Details** | Consolidated Bill

Expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. Actual deduction amount will be in 2 decimal places. For more details, see User Guide Current Bills.

All products | Please choose one product | Please choose one subproduct | All Projects | All Regions | All AZs

All Billing Modes | All transaction types | ☐ Do not display \$0 transactions

Total Cost (Including Tax) **248.01491871 USD** = Total Amount After Discount (Excluding Tax) **239.86954595 USD** - Voucher Deduction **10.22607970 USD** + Tax Amount **18.37145246 USD**

| Instance ID | Instance Name | Product Name | Payer Account ID | Owner Account... | Operator Account ID | Billing Mode | Instance Type |
|-----------------------|---------------|----------------------|------------------|------------------|---------------------|-------------------------|---------------|
| disk-g3vjdt8 | Unnamed | cloud block storage | | | | Monthly subscription | - |
| disk-alut2mki | Unnamed | cloud block storage | | | | Monthly subscription | - |
| disk-o37xsgum | Unnamed | cloud block storage | | | | Monthly subscription | - |
| 100010445724-std_r... | | Cloud Object Storage | | | | Pay-As-You-Go resources | - |
| 100010445724-std_s... | | Cloud Object Storage | | | | Pay-As-You-Go resources | - |

Consolidating Member Account Bills

This section describes how the admin account consolidates the bills of multiple member accounts.

Directions

1. Log in to the **Billing Center** console with the admin account and select **Bill Details** on the left sidebar.
2. Select the **Consolidated Bill** tab, select the member accounts for which you want to consolidate bills, and click **Download Consolidated Bill**. You can also go to the **Download Records** page and click **Download** to download the consolidated bills.

Billing Center

Bill Details 2023-02

Bill by Instance | Bill Details | **Consolidated Bill**

Expense figures in Bill Details are accurate up to 8 decimal places. Expense figures in Bill by Instance are rounded off to 2 decimal places. Actual deduction amount will be in 2 decimal places. For more details, see User Guide Current Bills.

| <input type="checkbox"/> Account ID | Customer Name | Total Amount After Discount (USD) |
|-------------------------------------|---------------|-----------------------------------|
| <input checked="" type="checkbox"/> | | 258.24 |
| <input type="checkbox"/> | | 0.00 |
| <input type="checkbox"/> | | 0.00 |
| <input type="checkbox"/> | | 0.00 |
| <input type="checkbox"/> | | 0.00 |
| <input type="checkbox"/> | | 0.00 |

[Download Consolidated Bill](#)

Issuing Invoices to Member Accounts

This section describes how the admin account issues invoices to member accounts.

Directions

1. Log in to the **Billing Center** console with the admin account and select **Invoicing** on the left sidebar.
2. In the drop-down list in the top-right corner, select a member account to issue the invoice. The issued invoice belongs to the member account.

Invoice

242753776@qq.cc

Invoice Settings

Invoice Title *

Email *

Please select ▼

Auto Invoicing

☐

After you enable this, the system will invoice the bills of the last month on the 6th day of the current month and send the invoice to your email address in 3 to 5 days.

Save

Invoice History

You can request for invoicing or download bills of the last 6 months.

| Billing Period | Application Time | Invoice Status | Invoiced Amount (USD) | Operation |
|----------------|------------------|----------------|-----------------------|-----------|
|----------------|------------------|----------------|-----------------------|-----------|

Inheriting Offers

This section describes how a member account inherits the admin account's offers specified in the contract.

Inheritable offers

Member accounts can inherit the contract offers applied for by the sales rep, but not the official discount or promotional discount.

Contract offers include **billing-level offers**, **finance-level offers**, and **rebates**, as detailed in the table below:

| Offer Type | Billing-Level Offer | Finance-Level Offer | Rebate |
|-------------------|---|---|--|
| Offer description | It is applied to a single prepaid or pay-as-you-go order and takes effect in real time. | It is applied to consolidated bills on a monthly basis and takes effect on the first day of the next month. | It is a rebate (in the form of voucher or free credit) calculated based on a certain proportion of the bill amount in the current month. It takes effect on the third day of the next month. |
| Discount | ✓ | × | × |
| Contract price | ✓ | × | × |

| | | | |
|---|---|---|---|
| (linear, tiered, or fixed pricing) | | | |
| Minimum spend (fixed or fluctuated monthly) | × | × | × |

Note:

“✓” means the offer is inheritable, and “×” means uninheritable.

Note:

1. Make sure all offers of member accounts are covered by the ones the admin account has applied for, so that they can still enjoy those offers after inheriting from the admin. Member accounts can choose to use their own applied offers without inheriting the admin account's offers, but once they inherit, only the inherited offers will apply.
2. Inherited offers cannot be applied to products in the blocklist which don't support offer inheritance.
3. Only when the member accounts and the admin account use the same settlement cycle (such as daily or monthly) can the former inherit the latter's offers. You can adjust the settlement cycle of products such as Cloud Streaming Services, Video on Demand, and Short Message Service for member accounts through CPQ.
4. Rebates and finance-level offers cannot be inherited.

You can go to the TCO console to allow **member accounts under the same verified entity as yours** to inherit your offers. To implement offer inheritance for **member accounts under a different verified entity**, contact your sales rep. Once the inheritance relationship is established, you can view the inheritance details of your member accounts.

In the organization fund allocation or member self-pay mode, the inherited offers will remain effective when the admin deletes the organization or removes organization members, or when members actively quit the organization. To cancel these offers, contact your sales rep.

Directions

Setting offer inheritance

When adding a member, you can set offer inheritance for the member account as follows:

1. Log in to the TCO console and click [Member account management](#) on the left sidebar.
2. On the **Member account management** page, click **Add member**.
3. On the **Add member** page, set offer inheritance in different ways based on different member adding methods.

Create member: The created member account and the admin account are under the same verified entity by default.

Select **Self-pay** for the **Payment mode** option, select **Inherit offer**, and fill in other required information to create the member.

Adding method

Create member
Create a Tencent Cloud root account and add it to the organization

Invite member
Invite a Tencent Cloud root account that is in use to join the organization

Member name *

The name must be unique in the organization and can contain 1-25 letters, digits, Chinese characters, or symbols (@, &_[]-;.).

Entity ①

Current entity

Other entities

Name of the current verified entity: 深圳市腾讯计算机系统有限公司

Finance permission

☒ View bills

☒ View balance

☒ Aggregate payments

☐ Invoice

Payment mode

Self-pay

Pay-on-behalf

Payer

787000128@qq.com

Before you pay on behalf of other accounts, make sure your account balance is sufficient. For details, see [here](#).

Department

Root

Create department

After a member account is successfully created, its verified identity will be the selected entity. An admin role will be created for the created account based on the selected access permission and then granted t

OK

Cancel

Invite member:

If the member account and the admin account are under the same verified entity, select **Self-pay** for the **Payment mode** option, select **Inherit offer**, and fill in other required information to invite the member.

Adding method

Create member

Create a Tencent Cloud root account and add it to the organization

Invite member

Invite a Tencent Cloud root account that is in use to join the organization

Account ID *

Please enter the ID of the Tencent Cloud account you w

You can invite a Tencent Cloud account that has the same verified identity as yours.

Member name *

Please enter the member name

It can only contain 1-25 letters, digits, Chinese characters, and symbols (@, & _ [] -:.).

Finance permission

Finance management

☒ View bills

☒ View balance

☒ Aggregate payments

☐ Invoice

Payment mode

Self-pay

Pay-on-behalf

☐ Inherit offer

Department

Root

Create department

Active quitting supported

☒ If this option is enabled, the member account can actively quit the organization.

The invited account must either accept or reject the invitation within 15 days; otherwise, the invitation will expire.

OK

Cancel

If the member account and the admin account are under different verified entities, contact your sales rep if you want to set offer inheritance after selecting **Self-pay** for the **Payment mode** option.

Canceling inherited offers

To cancel the inherited offers of member accounts, contact your sales rep.

Member Access Management

Service Control Policy

Overview

Last updated : 2024-03-06 18:52:29

A service control policy in TCO is an access control policy based on a hierarchical structure (department and member). It can uniformly manage the access permission boundaries of resources at each level within an organization and thus establish global or local access control rules. It only defines the permission boundaries and does not actually grant permissions. You still need to set permissions in CAM for a member account to access certain resources.

Use cases

After you create an organization and create members under each department, if you don't control the behaviors of members, the Ops rules will be violated, causing security risks and increasing costs. TCO provides the service control policy feature. You can centrally create management rules through account management and apply them to different structure levels such as departments and members. This enables you to better manage the access rules of resources for members, ensure the security compliance, and control costs. For example, you can use this feature to forbid a member from applying for domain names or deleting logs.

Service control policy types

System service control policy

This type refers to the service control policies that are preset in the system. You can view them but cannot create, modify, or delete them. After the service control policy feature is enabled, all departments and members in your organization are bound to the system policy `FullQcloudAccess` by default, which allows them to perform any operations on all your Tencent Cloud resources.

Custom service control policy

This type refers to the service control policies that you customize. You can create, modify, and delete such policies. After creating a custom policy, you need to bind it to a department or member for it to take effect. You can also unbind it at any time.

How a service control policy works

1. Enable the service control policy feature with the admin account as instructed in [Enabling Service Control Policy](#).
2. After the service control policy feature is enabled, the system policy `FullQcloudAccess` will be bound to all departments and members in your organization by default. This policy allows all actions in order to avoid access failures caused by improper policy configuration.
3. Create a service control policy with the admin account as instructed in [Creating Custom Service Control Policy](#).
4. Bind the service control policy to an organization node such as department or member with the admin account as instructed in [Binding Custom Service Control Policy](#).
5. A service control policy can be bound to departments and members in the organization and can be inherited by lower nodes. For example, if you set service control policy A for the parent department and policy B for a child department, both policies A and B will take effect for the child department and its members.

Note:

Perform a local test first to ensure that the policy works as expected before binding it to all target nodes such as departments and members.

6. When a CAM user or role among members accesses a Tencent Cloud service, Tencent Cloud will first check its associated service control policies and then check CAM permissions under the account as follows:
 - (1) Authentication with service control policies starts from the account of the accessed resource and continues upward level by level in the organization.
 - (2) If the action is denied by a service control policy at a level, the authentication result will be "Explicit Deny", the entire authentication process will end, authentication with the account's CAM permission policies won't be performed, and the request will be directly denied.
 - (3) If the action is neither denied nor allowed by a service control policy at a level, the authentication result will also be "Explicit Deny", authentication won't proceed to the next level, the entire authentication process will end, authentication with the account's CAM permission policies won't be performed, and the request will be directly denied.
 - (4) If the action hits an allow policy at a level, authentication will pass at this level and proceed to the parent node until the root. If authentication at the root level also passes, the entire authentication will pass, and authentication with the account's CAM permission policies will be performed.
 - (5) Service control policies don't take effect for the service's associated roles.
 - (6) Tencent Cloud will assess the service control policies of the accessed account as well as those bound to its nodes at each level, so as to ensure that the policies bound to nodes at a higher level can take effect for all accounts under it.

Enabling Service Control Policy

Last updated : 2024-03-06 18:52:29

The service control policy feature is disabled by default. You need to enable it before using it.

Background

After the service control policy feature is enabled, your organization will have the following changes:

All departments and members in your organization are bound to the system policy `FullQcloudAccess` by default, which allows them to perform any operations on all your Tencent Cloud resources.

When a department or member is created, it will be automatically bound to the system policy

`FullQcloudAccess` .

After a Tencent Cloud account accepts the invitation to join your organization, it will be automatically bound to the system policy `FullQcloudAccess` .

When a member is removed, all service control policies bound to it will be unbound automatically.

Directions

1. Log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > **Service control policy**.
3. Toggle on **Service control policy**.

Subsequent steps

You can create a custom service control policy (such as denying an operation on a resource) and bind it to a department or member in your organization. For detailed directions, see the following documents:

[Creating Custom Service Control Policy](#)

[Binding Custom Service Control Policy](#)

Creating Custom Service Control Policy

Last updated : 2024-03-06 18:52:29

You can create custom service control policies to restrict specified operations on specified resources and define the permissions boundary for departments and members in your organization.

Creation Methods

1. Create a custom service control policy in visual editing mode

The system offers an easy-to-use WYSIWYG editing page. You only need to select an effect, Tencent Cloud service, action (operation), resource, and condition to create a custom service control policy. In addition, it also offers a smart verification feature to help you guarantee the correctness and effectiveness of the policy.

2. Create a custom service control policy by editing a script

The system offers a JSON script editing page, where you can write a custom service control policy according to the policy syntax and structure. This method is flexible and suitable if you are familiar with the policy syntax.

Creating a custom service control policy in visual editing mode

1. Log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > **Service control policy**.
3. On the **Policy list** tab, click **Create policy**.
4. On the **Create policy** page, click the **Visual policy generator** tab.
5. Configure the service control policy and click **Next** to edit basic information.

In the **Effect** section, select **Allow** or **Deny**.

In the **Service** section, select a Tencent Cloud service.

Note:

Only Tencent Cloud services displayed on the page support the visual editing mode.

In the **Action** section, select **All actions** or **Custom action**.

The system automatically filters configurable actions based on the Tencent Cloud service selected in the previous step. If you select **Custom action**, you need to select specific actions.

In the **Resource** section, select **All resources** or **Specific resources**.

The system automatically filters configurable resource types based on the actions selected in the previous step. If you select **Specific resources**, you need to click **Add a six-segment resource description** and configure the specific resource ARN. You can click **Match all** to quickly select all resources corresponding to the configuration item.

(Optional) In the **Condition** section, click **Source IP** to configure a condition.

You can enter an IP (or IP range) or add other conditions, including Tencent Cloud general or service-level conditions. The system automatically filters configurable conditions based on the service and actions selected in previous steps.

You only need to select the condition keys to configure the specific content.

6. Enter the **Name** and **Description** of the service control policy and click **Complete**.

Creating a custom service control policy in JSON mode

1. Log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > **Service control policy**.
3. On the **Policy list** tab, click **Create policy**.
4. On the **Create policy** page, click the **JSON** tab.
5. Enter the content of the service control policy and click **Next** to edit basic information.
6. Enter the **Name** and **Description** of the service control policy.

Subsequent Steps

After creating the custom service control policy successfully, you need to bind it to a department or member for it to take effect. For detailed directions, see [Binding Custom Service Control Policy](#).

Viewing Service Control Policy Details

Last updated : 2024-03-06 18:52:29

You can view information such as the service control policy name, type, content, and bound targets.

Directions

1. Log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > **Service control policy**.
3. On the **Policy list** tab, click **Policy name**.

In the **Basic information** section, view the **Policy name**, **Policy type**, and **Policy description**.

On the **Policy syntax** tab, view the policy content.

On the **Binding management** tab, view the departments and members bound to the policy.

Modifying Custom Service Control Policy

Last updated : 2024-03-06 18:52:29

You can modify the name, description, and content of a custom service control policy as needed. The modification will take effect immediately for the departments and members bound to the policy.

Background

System service control policies cannot be modified.

Directions

1. Log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > **Service control policy**.
3. On the **Policy list** tab, click the name of the target service control policy.
4. In the top-right corner of the **Policy details** page, click **Edit policy**.

Modify the content of the service control policy by using the visual policy generator or editing the JSON script. Then, click **Next** to edit basic information.

For detailed directions, see [Creating Custom Service Control Policy](#).

5. Modify the **Name** and **Description** and click **OK**.

Deleting Custom Service Control Policy

Last updated : 2024-03-06 18:52:29

You can delete custom service control policies not bound to any departments or members at any time.

Background

System service control policies cannot be deleted.

For a custom service control policy bound to a department or member, you need to unbind it before deleting it. For more information, see [Unbinding Custom Service Control Policy](#).

Directions

1. Log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > **Service control policy**.
3. On the **Policy list** tab, click **Delete** in the **Operation** column of the target service control policy.
4. Click **OK**.

Binding Custom Service Control Policy

Last updated : 2024-03-06 18:52:29

You can bind a custom service control policy to departments or members, which will be controlled by it immediately. Make sure that the result of the binding operation is as expected to avoid affecting the normal business operations.

Background

1. The system binds the system policy `FullQcloudAccess` to the resource folders and members by default.
2. A service control policy takes effect for the entire bound node; that is, a policy bound to a parent department also takes effect for child departments and their members.

Directions

1. Log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > **Service control policy**.
3. Click the name of the target policy to enter the policy details page and select **Binding management**.
4. Click **Bind**. In the pop-up window, select the target departments or members.
5. Click **OK**.

Unbinding Custom Service Control Policy

Last updated : 2024-03-06 18:52:29

You can unbind a custom service control policy at any time. Then, the originally bound departments or members will not be controlled by the policy. Make sure that the result of the unbinding operation is as expected to avoid affecting the normal business operations.

Background

Both system policies and custom service control policies can be unbound, but the last policy bound to a department or member cannot be unbound.

Directions

1. Log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > **Service control policy**.
3. Click the name of the target policy to enter the policy details page and select **Binding management**.
4. In the list, click the target department or member and click **Unbind**.
5. Click **OK**.

Disabling Service Control Policy

Last updated : 2024-03-06 18:52:29

If you don't want to restrict the permissions of departments and members in your organization, you can disable the service control policy feature.

Background

After the service control policy feature is disabled, all policies bound to departments and members will be unbound automatically. The policies won't be deleted, but they can no longer be bound to any target objects.

Note:

Disabling the service control policy feature will affect the permissions of all departments and members in the organization. Perform this operation with caution.

Directions

1. Log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > **Service control policy**.
3. At the top of the **Service control policy** page, click **Disable service**.
4. Click **OK**. If the status becomes **Control policy disabled**, the feature has been disabled.

Note:

You can also click **Enable service control** to enable the service control policy feature again. Then, the system policy `FullQcloudAccess` will be automatically bound to all departments and members by default, but custom policies need to be manually bound again.

Resource Management

Organization Service Management

Overview

Last updated : 2024-03-06 18:52:29

Organization service management is the process of managing TCO-enabled Tencent Cloud services. TCO allows these Tencent Cloud services to access the department and member information in the TCO console. You can use the admin account or delegated admin account to manage the organization business in the console of each TCO-enabled product to simplify the unified management of your cloud business.

Directions

You can use the organization service management feature **in the TCO console or through APIs**. Below are the **console** directions.

1. In the [TCO console](#), use the admin account to activate the TCO service. For directions, see [Creating Organization](#).
2. In the [TCO console](#), use the admin account to build the organization structure. You can create members or invite existing Tencent Cloud accounts to join the organization. For directions, see [Creating Department](#) and [Adding Organization Member](#).
3. (Optional) In the [TCO console](#), use the admin account to specify a member as the delegated admin of the organization service management. If you don't specify a delegated admin, you need to use the admin account to manage your business in the TCO-enabled product console. For more information, see [Managing Delegated Admin Account](#).

Note :

This step only applies to the scenario where the delegated admin is supported.

4. In the [TCO console](#), use the admin or delegated admin account to enable the multi-account management feature. Select members that need to be managed in a unified manner based on the organization structure and manage business for the selected members.

Enabling/Disabling Organization Service Management

1. You can enable or disable the organization service management feature in the consoles of the TCO-enabled products or through APIs.
2. You can go to the [Organization service management](#) page to view whether this feature is enabled. However, you cannot enable or disable this feature in the TCO console.

3. For some TCO-enabled products, when you perform certain operations, the status of the organization service management feature will be automatically updated to "Enabled".
4. The feature status will be automatically updated to "Disabled" when you perform operations such as disabling a feature. If you disable organization service management for a TCO-enabled product, the product cannot access the organization accounts or resources in TCO, and all TCO-related resources will be deleted from the product.

Organization service management and service-linked role

1. TCO has created a service-linked role `TencentCloudServiceRoleForOrganizations` for each member. This role allows TCO to create roles for a TCO-enabled product. This role can only be played by TCO.
2. The TCO-enabled product only creates service-linked roles for members who need to perform admin operations. This role defines the permissions with which the TCO-enabled product can perform certain operations. It can only be played by the corresponding TCO-enabled product.
3. The permission policy of the service-linked role is defined and used by the corresponding cloud service. You cannot modify or delete the permission policy, nor can you add or remove permissions for the service-linked role.

Managing Delegated Admin Account

Last updated : 2024-03-06 18:52:29

This document describes the definition and use limits of the delegated admin account and its related operations.

Definition

The organization admin account can specify a member account as the delegated admin account of a TCO-enabled product. With the admin account's authorization, the delegated admin account can access the TCO organization and member information and manage the organization business in the console of the TCO-enabled product.

After setting the delegated admin account, organization management tasks and business management tasks can be separated, as the admin account and the delegated admin account are in charge of organization management and business management respectively. This conforms to the best security practices.

Use limits

1. The delegated admin account can only be a member account rather than the organization admin account.
2. The number of delegated admin accounts that can be added is determined by each TCO-enabled product.

Adding delegated admin account

1. Use the admin account to log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > [Organization service management](#).
3. On the **Organization service management** page, click **Add** in the **Operation** column.
4. In the pop-up window, select one or multiple members as needed in the account selection area.
5. Click **OK**.

Note:

After the delegated admin account is added, you can use it to access the multi-account management module of the TCO-enabled product to perform related admin operations.

Removing delegated admin account

Note:

The removal operation may affect your normal use of the TCO-enabled product. Proceed with caution.

1. Use the admin account to log in to the [TCO console](#).
2. On the left sidebar, select **Organization account** > [Organization service management](#).
3. On the **Organization service management** page, click the number in the **Delegated admin** column.
4. On the **Delegated admin** page, click **Remove** in the **Operation** column of the target account.
5. Confirm the note in the dialog box and click **Continue**.

Note :

After the delegated admin account is successfully removed, it cannot access the TCO organization and member information in the TCO-enabled product console.

Member Audit

Auditing Member Log

Last updated : 2024-03-06 18:55:02

The TCO admin can ship the logs of organization members to the specified location through a tracking set in CloudAudit.

Identity Center Management

Introduction to Identity Center

Introduction to Identity Center

Last updated : 2024-07-31 14:17:23

Identity Center provides unified identity and permission management for multiple accounts based on the organizational structure of organization accounts. Using the Identity Center feature of Tencent Cloud Organization (TCO), you can centrally manage the users who use Tencent Cloud in your enterprise, configure the enterprise identity management system with Tencent Cloud's single sign-on (SSO) in one go, and centrally configure user access permissions to multiple accounts.

Features

Centrally managing users who use Tencent Cloud

Identity Center offers you a user management module where you can maintain all users who need to access Tencent Cloud. You can manage users and user groups manually or use the System for Cross-domain Identity Management (SCIM) protocol to synchronize users and user groups from your enterprise identity management system to Identity Center.

Centrally configuring SSO with your enterprise identity management system

Identity Center supports enterprise-level SSO based on the Security Assertion Markup Language (SAML) 2.0 protocol. Only a one-time configuration in both Identity Center and the enterprise identity management system is needed to set up SSO.

Centrally configuring user access permissions for multiple accounts

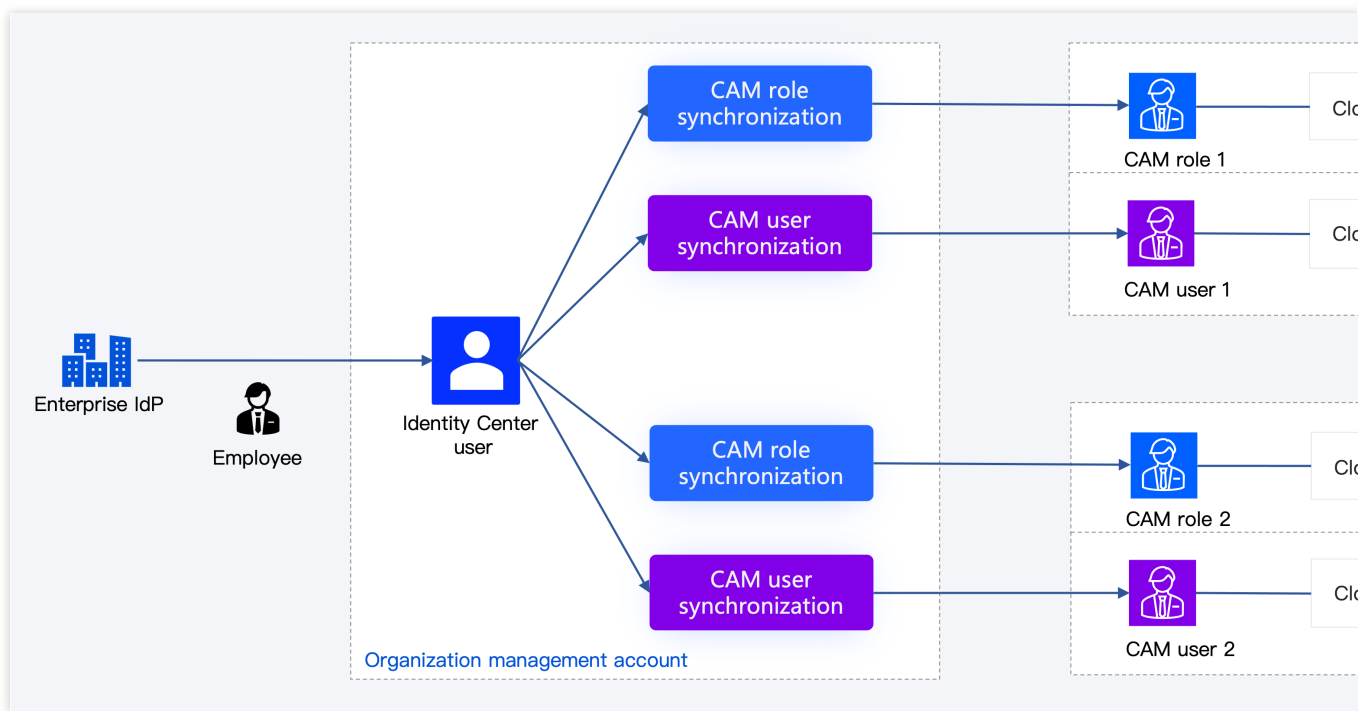
By leveraging the organizational structure of organization accounts, you can centrally configure user or user group access permissions to any member account within the enterprise in Identity Center. These permissions can be modified or deleted at any time.

Unified login portal

Identity Center provides a unified login portal where enterprise employees can access all accounts they are authorized to use with a single login. They can then log in to the Tencent Cloud console and easily switch between multiple accounts.

Product Architecture

Identity Center users can access cloud resources of an account through **Cloud Access Management (CAM) roles** or **CAM users**.



Note:

If the same Identity Center user is configured with both CAM role synchronization and CAM user synchronization through permission configuration on the account, the Identity Center user can access the account's cloud resources through both CAM roles and CAM users.

Relationship Between Identity Center and CAM

CAM provides identity and permission management within a single Tencent Cloud account. CAM offers user management (including users, user groups, and roles), SSO, and permission configuration, but these are only effective within one Tencent Cloud account. When your enterprise has multiple Tencent Cloud accounts, you need to use CAM in each account to manage users separately and to configure SSO and permissions separately, which poses significant management challenges.

Identity Center provides unified identity and permission management across multiple accounts within an organization. With Identity Center, you can perform unified configuration once, achieving user management, SSO, and permission configuration for multiple Tencent Cloud accounts. To achieve this, Identity Center offers identity management independent of CAM, but its permission configuration reuses the permission policies in CAM. Additionally, the access of Identity Center users to accounts is essentially another SSO performed by Identity Center users assuming the CAM role in each account.

When you start using Identity Center for unified identity and permission management across organization accounts, you will no longer need to use CAM to manage individual accounts. However, in certain cases, such as when you have existing CAM users and CAM roles, or need to use access keys for programmatic access to Tencent Cloud resources, you can still use CAM within individual accounts. Using Identity Center does not restrict the original features of CAM; both services can be used simultaneously.

Basic Concepts

Last updated : 2024-07-31 14:17:23

This document introduces the basic concepts of Identity Center.

| Concept | Description |
|-------------------------------------|--|
| Space | When enabling Identity Center, you need to create a space. All Identity Center resources are maintained within the space. An organization account can create only one space. The space name will be used in the user login URL. |
| User | User is a type of identity in the Identity Center. It refers to new users you create in the Identity Center after you enable the Identity Center service of organization accounts. Before CAM synchronization, users in the Identity Center do not have any feature, identity, login permission, access permission, etc. You can create and manage all users accessing Tencent Cloud here. Users can be granted permissions to access Tencent Cloud accounts. |
| User Group | User group is a type of identity in the Identity Center. You can add users to a user group and then grant permissions based on the user group for unified permission management. |
| SCIM Synchronization | The Identity Center supports user and user group synchronization based on the System for Cross-domain Identity Management (SCIM) protocol. By using SCIM synchronization, you can manage identities in your enterprise identity management system without manually managing users, user groups, and their memberships in the Identity Center, enhancing management efficiency and security. |
| Permission Configuration | Permission configuration is a configuration template used by users to access Tencent Cloud accounts and includes a set of permissions. You can use this template to authorize users for specific accounts. |
| Account | Accounts include admin accounts and member accounts. Admin account: The admin account is the super administrator of the enterprise, and only the admin account can manage the Identity Center. Member account: Member accounts cannot manage the Identity Center, nor can they view it. |
| Multi-Account Authorization | Based on the organizational structure of the organization accounts, you can set the users or user groups allowed to access each account, as well as their access permissions. You can authorize enterprise admin accounts or any member account. |
| Permission Configuration Deployment | When you authorize users for an account, the specified permission configuration will be deployed to the relevant account, becoming the CAM role, CAM policy, and identity provider for role single sign-on (SSO) for that account. If the permission configuration has already been deployed to an account but changes are made to the permission |

| | |
|-------------------------------|--|
| | configuration, these changes will not be automatically updated to the account. You need to manually redeploy for the changes to take effect. |
| Login Portal | The login portal is an independent portal for Identity Center users to log in and use Tencent Cloud resources. After Identity Center users log in, they can view the accounts they have access to and can only access the Tencent Cloud console within the granted permissions. You can view the login portal address (URL) on the overview page of the Identity Center. |
| Identity Center Administrator | An Identity Center administrator refers to a CAM user who has an Identity Center management account and permissions (QcloudOrganizationFullAccess) under the account. |
| Single Sign-On (SSO) | Identity Center supports SSO based on Security Assertion Markup Language (SAML) 2.0. Tencent Cloud is the service provider (SP), while the enterprise's identity management system is the identity provider (IdP). Through SSO, enterprise employees can use their IdP user identity to directly log in to the Identity Center. |

Activate Services

Last updated : 2024-07-31 14:17:23

You need to activate the Identity Center to use it. After activation, you can use this service for free.

Prerequisites

You have activated the Group Account Services and established the multi-account organizational structure of the enterprise.

Only the administrative account of the group account or a CAM user with permissions under the administrative account can activate the Identity Center. Details are as follows:

Administrative account (root account)

CAM user (sub-account)

You need to grant the preset policy QcloudOrganizationFullAccess to the CAM user in the administrative account. For specific operations, refer to [Sub-user Permission Settings](#).

Directions

1. Log in to [TCO Console](#).
2. In the TCO Console directory, click **Identity Center Overview**.
3. On the **Identity Center Overview** page, click **Activate Now**.
4. At the time of activation, fill in the **Space Name**. The name must be globally unique.

The Space Name will be used in the user login URL subsequently and cannot be modified.

During the space creation process, the Identity Center will automatically create a service-related role (Orgnization_QCSLinkedRoleInCIC) to access your resources in other cloud services.

5. Click **OK**.

Manage Users

Last updated : 2024-07-31 14:17:23

Overview

This document introduces the basic operations for managing users, including creating a user, viewing user information, modifying basic user information, deleting a user, and enabling or disabling user login.

Prerequisites

You have logged in to **TCO** > [Identity Center](#).

Directions

Creating a User

1. In the left sidebar, select **User Management > Users**.
2. On the **Users** list page, click **Create User**.
3. On the **Create User** panel, set basic user information.

User Information

| Username* | Remarks | Last Name | First Name |
|----------------------|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

(Up to 10 users can be created at a time.)

Username: required. It must be unique within the space, and can include letters, numbers, and +=,.,@- _ characters, with a maximum length of 64 characters.

Remarks, Last name, First Name, Email: optional. You can enter these as needed.

4. Click **OK**.

Viewing User Information

1. In the left sidebar, select **User Management > Users**.

2. On the **Users** list page, click the target username to view the following information:

View basic user information.

Click the **User Groups** tab to view the user groups that the user has joined.

Click the **Security Information** tab to view the user's enabling status.

Click the **CAM User Synchronization** tab to view the configured CAM user synchronization information. For more information about CAM user synchronization, refer to [Multi-account Authorization Overview](#).

Click the **Permissions** tab to view the user's associated accounts and permissions configuration information.

Modifying Basic User Information

Note:

When the user source is SCIM synchronization, the basic information of the SCIM synchronized user cannot be modified.

The username cannot be modified.

1. In the left sidebar, select **User Management > Users**.

2. On the **Users** list page, click the target username.

3. In the **Basic Information** area at the top of the user **Details** page, the fields that can be modified are: **Remarks**, **Last name**, **First Name**, **Email**.

The screenshot shows the 'User Details' page. At the top, there's a navigation bar with a back arrow and the title 'User Details'. Below this is a section titled 'Basic Information' containing fields for Username, User ID, Email, Source (set to 'Create Manually'), Remarks, and Creation Time (2024-07-29 16:09:09). Below the 'Basic Information' section are four tabs: 'User Group', 'Security Information', 'CAM User Synchronization', and 'Permissions'. The 'User Group' tab is active, showing a table with columns for 'User Group Name', 'Join Time', and 'Source'. The table is currently empty, displaying 'No data available'. At the bottom of the 'User Group' tab, it says '0 item(s) selected, with a total of 0 item(s)'.

Deleting a User

Note:

When the user source is SCIM synchronization, the SCIM synchronized user cannot be deleted.

Before deleting a user, make sure that the user is not associated with the following resources; otherwise, the deletion will fail. Details are as follows:

User group: You need to remove the user from the user group. For specific steps, refer to [Remove User from User Group](#).

Permissions: You need to delete the user's authorization on the account. For specific steps, refer to [View/modify/delete authorization](#).

CAM user synchronization: You need to delete the user's synchronization relationship on the account. For specific steps, refer to [View/Modify/Delete User Synchronization](#).

1. In the left sidebar, select **User Management > Users**.
2. On the **Users** list page, click **Delete** in the target user's action column.
3. On the **Delete User** page, click **OK**.

Enabling or Disabling User Login

Warning:

Users in disabled status will not be able to log in to the Identity Center's login portal.

1. In the left sidebar, select **User Management > Users**.
2. On the **Users** list page, click the target username.
3. In the **Security Information** area of the details page, enable or disable user login.

The screenshot displays the 'User Details' page. At the top, there's a back arrow and the title 'User Details'. Below this is a 'Basic Information' section with fields for Username, User ID, Email, Source (set to 'Create Manually'), Remarks, and Creation Time (2024-07-29 16:09:09). Below the basic information is a tabbed interface with four tabs: 'User Group', 'Security Information' (which is active), 'CAM User Synchronization', and 'Permissions'. Under the 'Security Information' tab, there is a section for 'Enabled State' which is currently set to 'Enabled' with an edit icon.

Enable user login

In the **Manage User Status** pop-up window, click **Enable**, and then click **OK**.

Disable user login

In the **Manage User Status** pop-up window, click **Disable**, and then click **OK**.

Manage User Groups

Last updated : 2024-07-31 14:17:23

Overview

This document introduces the basic operations of user groups, including creating a user group, viewing user group information, modifying basic user group information, deleting a user group, adding a user to a user group, and removing a user from a user group.

Prerequisites

You have logged in to **TCO** > [Identity Center](#).

Directions

Creating a User Group

1. In the left sidebar, select **User Management** > **User Groups**.
2. On the User Groups page, click **Create User Group**.
3. On the **Create User Group** panel, enter **User Group Name**.

The User Group Name must be unique within the space.

4. Enter **Remarks** information.
5. Click **OK**.

Viewing User Group Information

On the **User Groups** list page, click the target user group name to view the following information:

View basic user group information.

Click the **Users** tab to view users in the user group.

Click the **CAM User Synchronization** tab to view the configured CAM user synchronization information.

Click the **Permissions** tab to view the associated accounts and permissions configuration information of the user group.

Modifying User Group Information

Note:

When the user group source is SCIM synchronization, the basic information of the SCIM synchronized user group cannot be modified.

1. On the **User Groups** list page, click the target user group name.
2. In the **Basic Information** area at the top of the **User Group Details** page, the fields that can be modified are: **User Group Name** and **Remarks**.

User Group Details

Basic Information

User Group Name

User Group ID

Creation Time

2024-07-12 14:25:49

Update Time

2024-07-12 14:25:49

Remarks

-

User

CAM User Synchronization

Permissions

Add User

Remove Users

Username

Join Time

Status

Source

No data available

Deleting a User Group

Before deleting a user group, make sure the user group is not associated with the following resources, otherwise the deletion will fail. Details are as follows:

Users: You need to remove users from the user group.

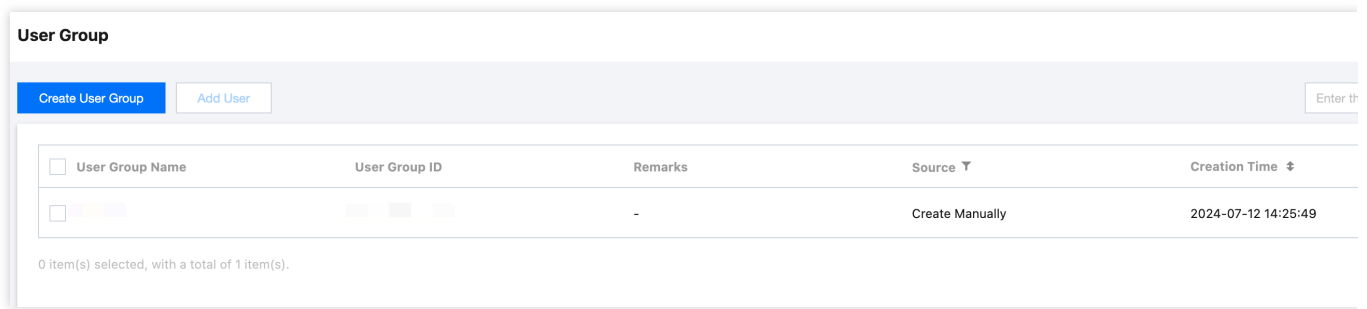
Permissions: You need to delete the user group's authorization on the account.

CAM user synchronization: You need to delete the synchronization relationship of the user group on the account.

Note:

When the user group source is SCIM synchronization, the SCIM synchronized user group cannot be deleted.

1. On the **User Groups** page, click **Delete** in the **Operation** column of the target user group.



2. In the **Delete User Group** dialog box, click **OK**.

Adding a User to a User Group

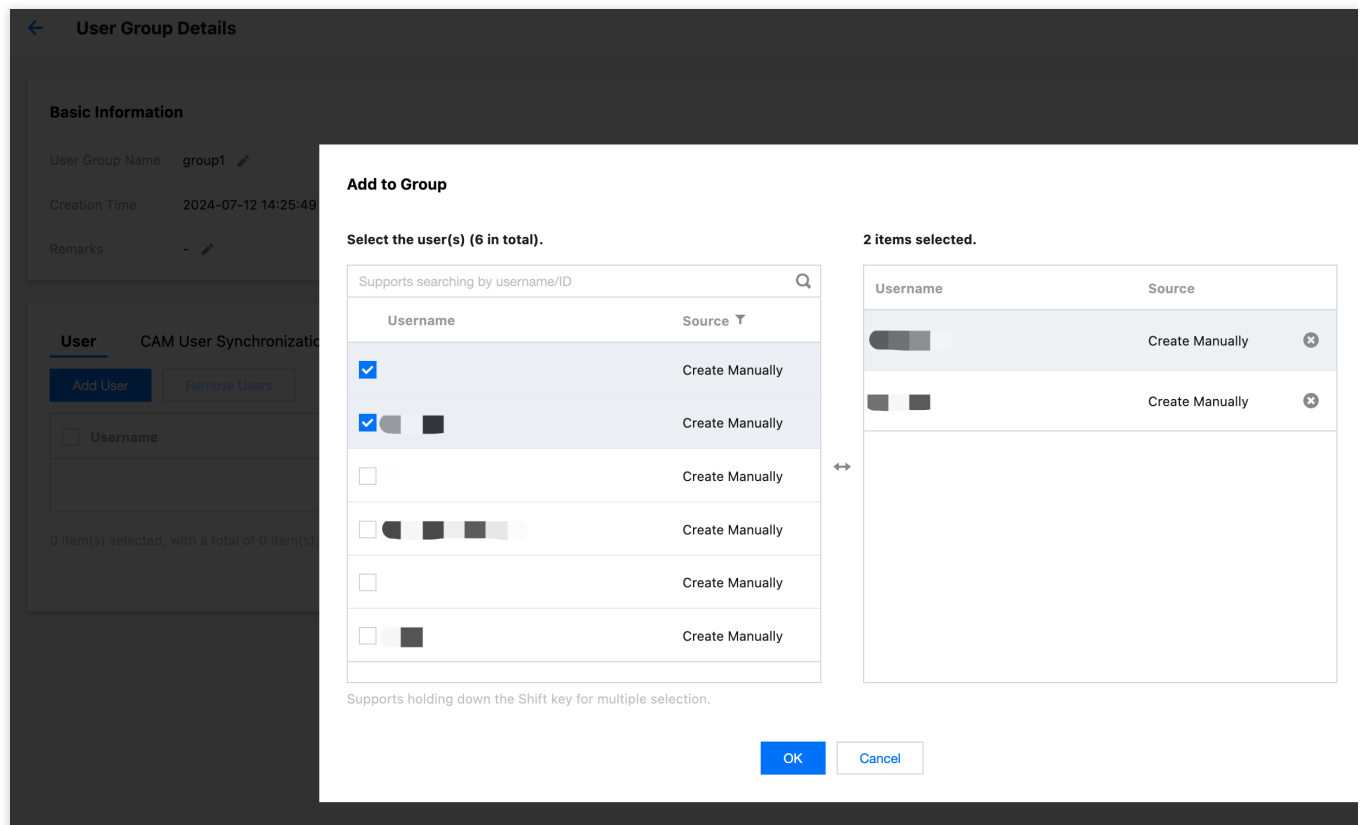
Note:

When the user group source is SCIM synchronization, a user cannot be added to the SCIM synchronized user group.

1. On the **User Groups** page, click the target user group name.
2. Click the **Users** tab, and then click **Add User**.
3. On the **Add to Group** panel, select **User**.

Note:

A user can join multiple user groups.



4. Click **OK**.

Removing a User from a User Group

Note:

When the user group source is SCIM synchronization, a user cannot be removed from the SCIM synchronized user group.

1. On the **User Groups** page, click the target user group name.
2. Click the **Users** tab.
3. Click **Remove from Group** in the **Action** column of the target user.
4. In the Remove User dialog box, click **OK**.

Settings

Manage SSO

Last updated : 2024-07-31 14:17:23

Overview

The TCO Identity Center supports SAML 2.0-based single sign-on (SSO). Tencent Cloud is a service provider (SP), and the enterprise's own identity management system is an identity provider (IdP). Through SSO, enterprise employees can use users in the IdP to directly log in to the Identity Center.

Directions

Enabling SSO

1. Log in to the **TCO > Identity Center Management > Settings > SSO** page. After enabling SSO, you can configure identity provider information.

Note:

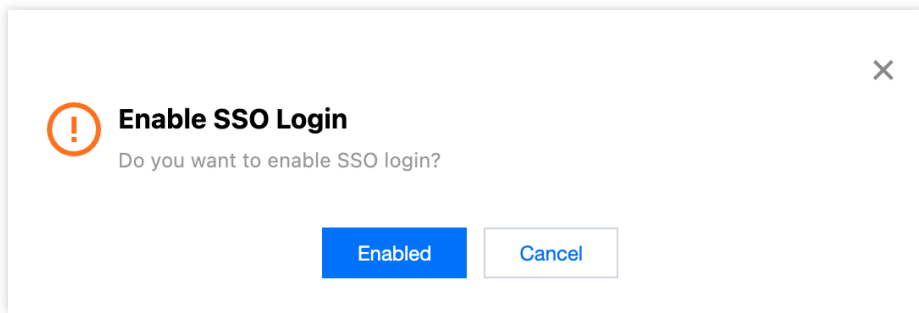
Currently, only SSO is supported, and username and password login is not supported.

2. In the **SSO Login** area, turn on the SSO switch.

Settings

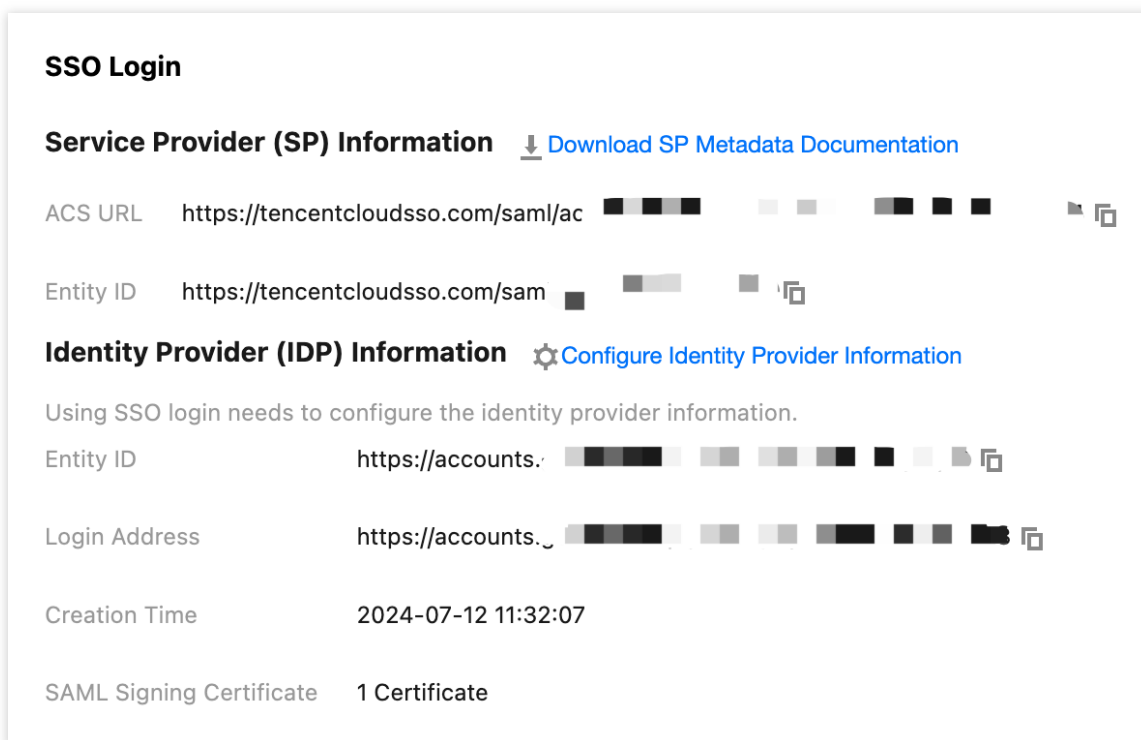
SSO Login

3. In the **Enable SSO Login** dialog box, click **Enabled**.



Managing Service Provider (SP) Information

When configuring SSO in an external IdP, you will need the SP metadata file. You can download the SP metadata file by clicking **Download SP Metadata Documentation** in the **Service Provider (SP) Information** area of the **TCO > Identity Center Management > Settings > SSO Login** page. You can also view or copy **ACS URL** and **Entity ID** for manual configuration in an external IdP.



Managing Identity Provider (IdP) Information

You need to configure identity provider (IdP) information and enable the SSO switch to use the SSO feature normally. Both manual configuration and metadata file upload are supported to configure identity provider information. Manual configuration can only be used to configure essential attributes for SSO: Entity ID, Login Address, and SAML Signing certificate.

If you need to configure more IdP information, generate a metadata file on the IdP side and use the metadata upload method for configuration.

Configuring Identity Provider (IdP) Information

You need to configure identity provider information before enabling SSO.

1. You have logged in to **TCO** > [Identity Center](#).
2. In the left sidebar, click **Settings**.
3. In the **SSO's Identity Provider (IdP) Information** area, click **Configure Identity Provider Information**.
4. In the **Configure Identity Provider Information** dialog box, select **Upload Metadata Documentation** or **Configure Manually** to configure identity provider information.

You can choose either of the following two methods for configuration. Obtain the relevant metadata file or configuration information from your identity provider.

Upload Metadata Documentation

Click **Select File** to upload the identity provider's metadata documentation.

Configure Identity Provider Information

Configuration Method ☒ Upload Metadata Documentation ☐ Configure Manually

Upload File * [Select File](#)

Configure Manually

Configure Identity Provider Information

Configuration Method ☐ Upload Metadata Documentation ☒ Configure Manually

Entity ID *

Login Address *

Certificate * [Select File](#)

Entity ID: Identity provider identifier.

Login Address: Identity provider login address.

Certificate: a certificate used by the identity provider for SAML response signature. You can click **Select File** to upload the identity provider's certificate.

5. Click **OK**.

Updating Identity Provider (IdP) Information

You can update identity provider information whether SSO is enabled or disabled. However, for an update when SSO is enabled, inconsistencies between new and existing identity provider information may cause SSO failure. Proceed with caution.

1. In the **SSO's Identity Provider (IdP) Information** area, click **Configure Identity Provider Information**.
2. In the **Configure Identity Provider Information** dialog box, select the configuration method, modify the configuration information, re-upload the certificate or metadata file, and click **OK**.

Manage Permission Configuration

Overview of Permission Configuration

Last updated : 2024-07-31 14:17:23

Permission configuration is a configuration template used by Identity Center users to access accounts. It includes predefined policies of Cloud Access Management (CAM) and does not currently support custom policies. You can use this template to authorize Identity Center users on the account.

First Deployment of Permission Configuration

When you set permissions for users or user groups on the account, you need to specify a permission configuration. If no other users or user groups have been deployed with a permission configuration on that account, the Identity Center will deploy a permission configuration in the account's CAM for you. The deployment in CAM includes the following:

Create a **CAM role** of type **Identity Center synchronization**.

On the CAM role, bind the system policy specified in **permission configuration**. Custom policies are not currently supported.

If no authorizations have been made on the account, **create** an **identity provider**, allowing Identity Center users to use role single sign-on (SSO) to log in to the account.

You can view the aforementioned CAM role and identity provider in the CAM console of the account, but you **cannot modify** or **delete** them.

Redeploying Permission Configuration

If the permission configuration has already been deployed to an account but changes are made to the permission configuration, these changes will not be automatically updated to the account. You need to manually redeploy (add or delete system policies) for the changes to take effect.

Permission Configuration

Last updated : 2024-07-31 14:17:23

Overview

This document introduces how to create, view, and delete permission configuration, as well as how to add and delete a preset policy.

Directions

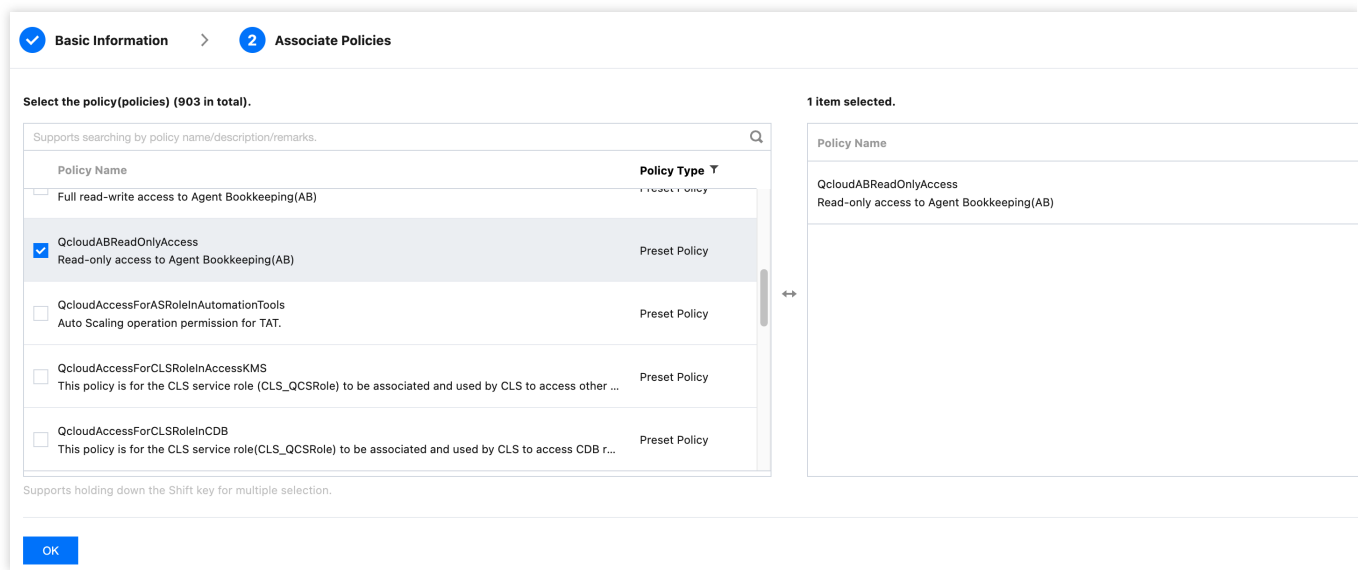
Creating Permission Configuration

1. You have logged in to **TCO** > [Identity Center](#).
2. In the left sidebar, click **CAM Synchronization** > **Configuring Permission**.
3. On the **Configuring Permission** page, click **Create Permission Configuration**.
4. On the **Create Permission Configuration** panel, configure the following basic information, and then click **Next**.

Permission Name: required parameter. It must be unique within the space.

Permission Description: optional parameter. It describes permission configuration.

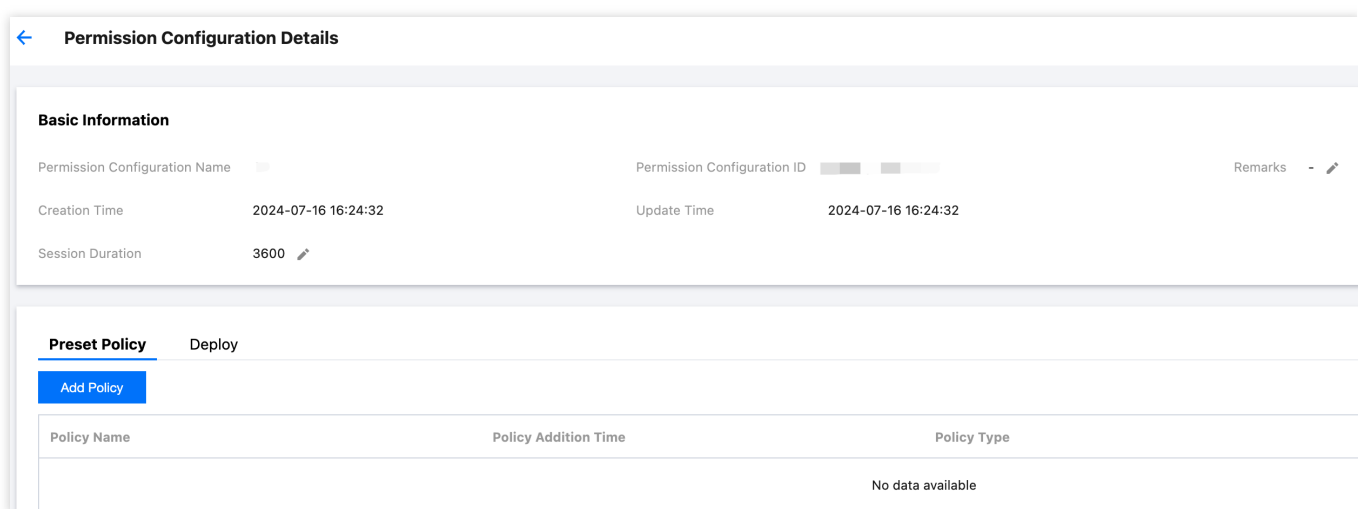
5. Configure associated policies, and select **Preset Policies** as needed.



6. Click **OK**.

Viewing Permission Configuration

1. You have logged in to **TCO** > [Identity Center](#).
2. In the left sidebar, click **CAM Synchronization** > **Configuring Permission**.
3. On the **Configuring Permission** page, click the target permission configuration name.
4. View the **Basic Information** of the permission configuration.
5. Click the **Preset Policy** tab to view preset policies for the permission configuration.



6. Click the **Deploy** tab to view member accounts that have been deployed under the permission configuration.

←

Permission Configuration Details

Basic Information

Permission Configuration Name

Permission Configuration ID

Remarks

Creation Time

2024-07-16 16:24:32

Update Time

2024-07-16 16:24:32

Session Duration

3600

Preset Policy

Deploy

Configure CAM Role Synchronization

Redeploy

| <input type="checkbox"/> Member Account Name/ID | Creation Time | Update Time | Deployment Status | Operati |
|---|---------------------|---------------------|----------------------|---------|
| | 2024-07-16 16:25:22 | 2024-07-16 16:25:22 | Succeeded to deploy. | Redepic |

0 item(s) selected, with a total of 1 item(s).

Deleting Permission Configuration

Prerequisites

Before deleting permission configuration, make sure that the permission configuration is not associated with the following resources:

Preset policies: You need to delete preset policies associated with the permission configuration.

Deployment: You need to undeploy the permission configuration in the member account.

Directions

1. You have logged in to **TCO** > [Identity Center](#).
2. In the left sidebar, click **CAM Synchronization** > **Configuring Permission**.
3. On the **Configuring Permission** page, click the **Operation** column of the target permission configuration and then click **Delete**.
4. In the **Delete Permission Configuration** dialog box, click **OK**.

Configuring Permission

CIC

① Permission Configuration is a set of permissions for users to access Tencent Cloud accounts. You can use this configuration to authorize users. When the configuration changes, you may need to redeploy to apply the changes.

Create Permission Configuration

Searchable Perm

Are yo
curren

| Permission Configuration Name | Description | Creation Time | Update Time | |
|-------------------------------|-------------|---------------------|---------------------|--------|
| test2 | - | 2024-07-30 11:27:51 | 2024-07-30 11:27:51 | Delete |

Adding or Deleting a Preset Policy

Note:

After adding or deleting a preset policy, if the permission configuration has already been deployed in the account, you need to redeploy the permission configuration for it to take effect in the account.

1. You have logged in to **TCO** > **Identity Center**.
2. In the left sidebar, click **CAM Synchronization** > **Configuring Permission**.
3. On the **Configuring Permission** page, click the target permission configuration name.
4. On the **Preset Policies** tab, add or delete a preset policy.

4.1 Add a preset policy

Click **Add Policy**.

The screenshot shows the 'Permission Configuration Details' page. Under the 'Basic Information' section, fields for 'Permission Configuration Name', 'ID', 'Creation Time', 'Update Time', and 'Session Duration' are visible. Below this, the 'Preset Policy' tab is active, showing an 'Add Policy' button highlighted with a red box. A table below the button is currently empty, with a 'No data available' message at the bottom.

On the **Add Preset Policy** panel, select **Preset Policies** as needed, and click **Add**.

Click **OK**.

4.2 Delete a preset policy

The screenshot shows the 'Permission Configuration Details' page with the 'Preset Policy' tab active. A confirmation dialog box is overlaid on the table, asking: 'Are you sure you want to delete the current associated policy? After the associated policy is deleted, accounts configured with this policy need to be re-deployed to take effect. Are you sure you want to continue deleting it?'. The dialog has 'OK' and 'Cancel' buttons. The table below shows a single row with a 'Delete' link in the 'Operation' column.

Click **Delete** in the **Operation** column of the target preset policy.

In the pop-up dialog box, click **OK**.

Redeploy Permission Configuration

Last updated : 2024-07-31 14:17:23

Overview

If the permission configuration has been deployed in the account, changes in the configuration will not be automatically updated to the corresponding account. You need to manually redeploy for the changes to take effect.

Prerequisites

When changes occur in the permission configuration (adding or removing a preset policy), you need to redeploy.

Directions

Redeploying the Permission Configuration on the Permission Configuration Page

1. Log in to **TCO** > [Identity Center](#).
2. In the left sidebar, click **CAM Synchronization** > **Configuring Permission**.
3. On the **Configuring Permission** page, click the target permission configuration name.

The system will automatically identify the permission configuration that needs redeployment, and its **Deployment Status** will be displayed as **Need to Be Redeployed**.

4. Click the **Deployment** tab.
5. Select the target account name.

The system will automatically identify the RD account that needs redeployment of access configuration, and its **Deployment Status** will be displayed as **Redeployment required**.

←

Permission Configuration Details

Basic Information

Permission Configuration Name

test1

Permission Configuration ID

Remarks

-

Creation Time

2024-07-12 14:26:13

Update Time

2024-07-12 14:26:13

Session Duration

3600

Preset Policy

Deploy

Configure CAM Role Synchronization

Redeploy

0 item(s) selected, with a total of 1 item(s).

6. Click **Redeploy**, confirm the following information on the **Redeploy** page, and click **Next**.

Redeploy

×

1 Confirm Redeployment

>

2 Redeploy

ⓘ

Confirm the permission configuration and member account to redeploy.

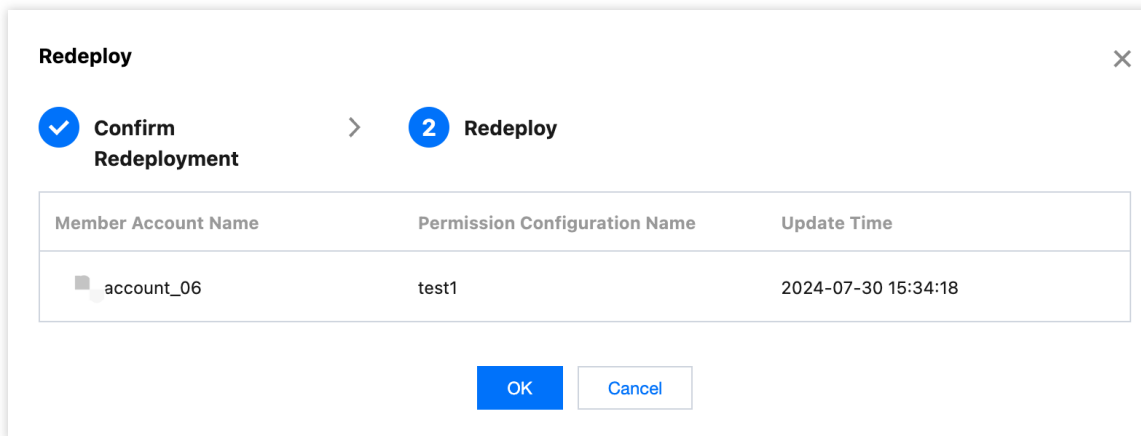
Permission Configuration Information

| Member Account Name | Permission Configuration Name | Update Time |
|------------------------|-------------------------------|---------------------|
| <div></div> account_06 | test1 | 2024-07-30 15:34:18 |

Next

Cancel

7. Click **OK**.

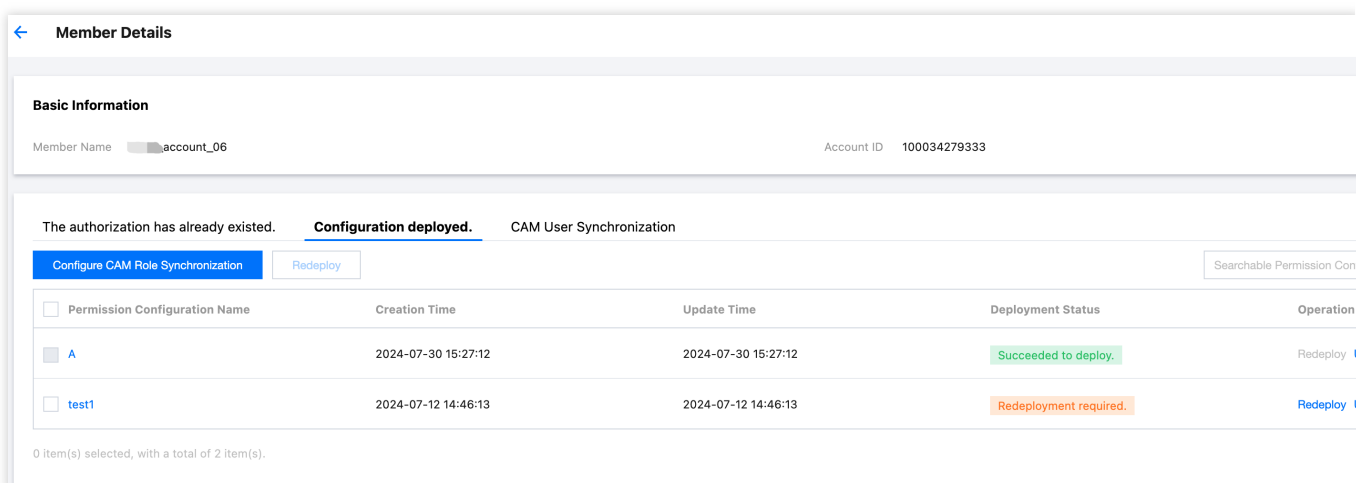


8. After deployment, the **Deployment Status** will be displayed as **Succeeded to deploy**.

Redeploying the Permission Configuration on the Multi-account Permission Management Page

1. Log in to **TCO > Identity Center**.
2. In the left sidebar, click **CAM Synchronization > Multi-account Permission Management**.
3. On the **Multi-account Permission Management** page, select the target account.
4. Click the **Deployed Configuration** tab.
5. Select the access configuration that needs to be redeployed.

The system will automatically identify the access configuration that needs redeployment, and its **Deployment Status** will be displayed as **Redeployment required**.



6. Click **Redeploy** and follow the on-screen instructions.
7. After deployment, the **Deployment Status** will be displayed as **Succeeded to deploy**.

Undeploy Permission Configuration

Last updated : 2024-07-31 14:17:23

Overview

You can proactively undeploy the permission configuration in an account. This document introduces how to undeploy the permission configuration.

Directions

Undeploying Permission Configuration on the Permission Configuration Page

1. Log in to **TCO** > [Identity Center](#).
2. In the left sidebar, click **CAM Synchronization** > **Configuring Permission**.
3. On the **Configuring Permission** page, click the target permission configuration name.
4. Click the **Deploy** tab.
5. Click **Undeploy** in the **Operation** column of the target account.

← Permission Configuration Details

Basic Information

| | | |
|-------------------------------|-----------------------------|---------|
| Permission Configuration Name | Permission Configuration ID | Remarks |
| Creation Time | Update Time | |
| Session Duration | | |

Preset Policy

Deploy

Configure CAM Role Synchronization

Redeploy

| Member Account Name/ID | Creation Time | Update Time | Deployment Status | Operation |
|------------------------|---------------------|---------------------|----------------------|-------------------|
| | 2024-07-16 16:25:22 | 2024-07-16 16:25:22 | Succeeded to deploy. | Redeploy Undeploy |

0 item(s) selected, with a total of 1 item(s).

6. In the **Undeploy** dialog box.

Confirm the authorization removal information, and click **Next** to remove the permission configuration from the user/user group.

Undeploy

1 Remove Authorization

>

2 Undeploy

>

3 Completed

Before the permission configuration is undeployed, you need to remove the authorization of the permission configuration in the account for the user/user group. Confirm the following authorization to be removed.

Associated Accounts

Account Name/ID

Associated Users/Groups

Associated Users/Groups

2 users; 0 user groups

Associated Users

Next

Cancel

Confirm the undeployment information, and click **Next** to undeploy the permission configuration in the account.

Undeploy

✓

1 Remove Authorization

>

2 Undeploy

>

3 Completed

Succeeded to remove the authorization of the user/user group for the following deployment. You can remove the deployment.

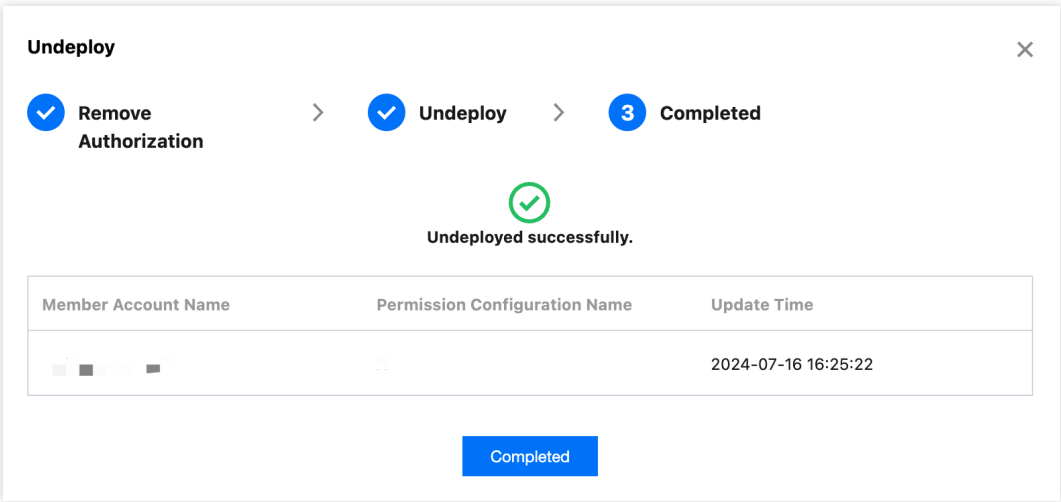
Permission Configuration Information

| Member Account Name | Permission Configuration Name | Update Time |
|---------------------|-------------------------------|---------------------|
| | | 2024-07-16 16:25:22 |

Next

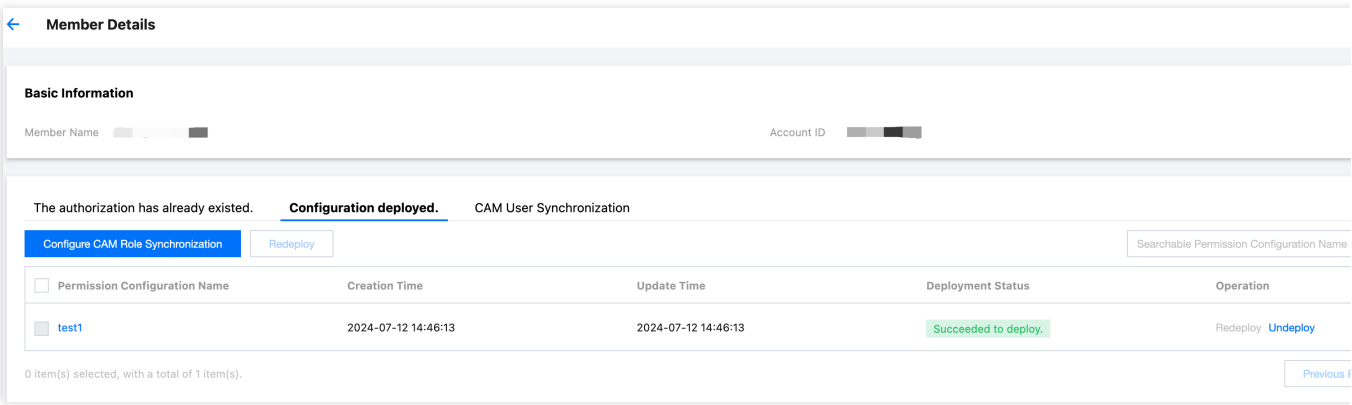
Cancel

Click **Completed**.



Undeploying Permission Configuration on the Multi-account Permission Management Page

- 1. Log in to TCO > Identity Center.
- 2. In the left sidebar, click CAM Synchronization > Multi-account Permission Management.
- 3. On the Multi-account Permission Management page, select the target account.
- 4. Click the Deployed Configuration tab.
- 5. Click Undeploy in the Action column of the target permission configuration.



- 6. Click Undeploy.
- Confirm the authorization removal information, and click **Next** to remove the permission configuration from the user/user group.
- Confirm the undeployment information, and click **Next** to undeploy the permission configuration in the account.
- Click **Completed**.

Manage Multi-account Authorization

Overview of Multi-Account Authorization

Last updated : 2024-07-31 14:17:23

On the multi-account authorization page, you can configure Cloud Access Management (CAM) user synchronization and CAM role synchronization based on the directory structure of the organization account.

Difference Explanation

Identity Center users can access the account's cloud resources through **CAM roles** or **CAM users**. The differences between the two methods are shown in the table below.

| Access Method | Description | Synchronization Method | Related Documentation |
|--------------------------------------|--|---|---|
| Configuring CAM Role Synchronization | Enterprises manage users accessing Tencent Cloud in the Tencent Cloud Organization's Identity Center. Through permission configuration and CAM role synchronization, users can log in to member accounts using single sign-on (SSO) and access the CAM roles within those accounts, and then access the cloud resources of the member account. | When configuring CAM role synchronization, the Identity Center will initiate tasks for each triplet (user-account-permission configuration). After synchronization, the access permissions in CAM are finalized and cannot be modified in CAM. | Permission Configuration Configuring CAM Role Synchronization |
| Configuring CAM User Synchronization | Enterprises manage users accessing Tencent Cloud in the Tencent Cloud Organization's Identity Center. Through CAM user synchronization, users can log in to member accounts and access the CAM users within those accounts, and then access the cloud resources of the member account. | When configuring CAM user synchronization, the Identity Center will initiate tasks for each tuple (user-account). After synchronization, the access permissions in CAM are empty and need to be configured in CAM. | Configuring CAM User Synchronization |

CAM Role Synchronization Explanation

If you need to perform a one-time batch authorization for multiple accounts, multiple identities, and multiple access configurations, you can go to **TCO > Identity Center**, enter the multi-account permission management page, view the account directory tree, and perform the following operations:

1. Select one or more accounts in the account tree as authorization targets.
2. Select one or more Identity Center identities.
3. Select one or more access configurations.
4. Click Configure CAM Role Synchronization, and the Identity Center service will complete the authorization for you in batches.

In batch authorization, if duplicate authorization is attempted for some existing authorizations, the operation will fail. However, newly added authorizations in the same batch will succeed.

Each time permissions are added, the Identity Center will initiate an asynchronous task for each triplet (identity-account-permission configuration).

CAM User Synchronization Explanation

If you need to perform a one-time batch authorization for multiple accounts and multiple identities, you can go to **TCO > Identity Center**, enter the multi-account permission management page, view the account directory tree, and perform the following operations:

1. Select one or more accounts in the account directory tree.
2. Select one or more Identity Center identities.
3. Click Configure CAM User Synchronization, and the Identity Center service will complete the synchronization for you in batches.

In batch synchronization, if a duplicate operation is attempted for some existing synchronizations, the operation will fail. However, newly added synchronizations in the same batch will succeed.

After successful configuration, a CAM user with the same name as the Identity Center user will be created in the target account.

Authorization: Access the target account to authorize the CAM user created in the previous step.

CAM users have no permissions by default. You need to grant them the appropriate permissions for the corresponding resources.

Identity Center users access the authorized resources in the target account through the CAM user identity.

For specific operations, see [Configuring CAM User Synchronization](#).

Configure CAM Role Synchronization

Last updated : 2024-07-31 14:17:23

Overview

Based on the group account organizational structure, you can set allowed access users or user groups for each account, as well as their permission configuration.

This document provides an example of deploying permission configuration on a member account (Account1) for a user (user1) from the Identity Center. The permission configuration defines access only to CVM, ensuring that the user (user1) from the Identity Center can only access CVM resources in the member account (Account1).

Prerequisites

Make sure you have created permission configuration.

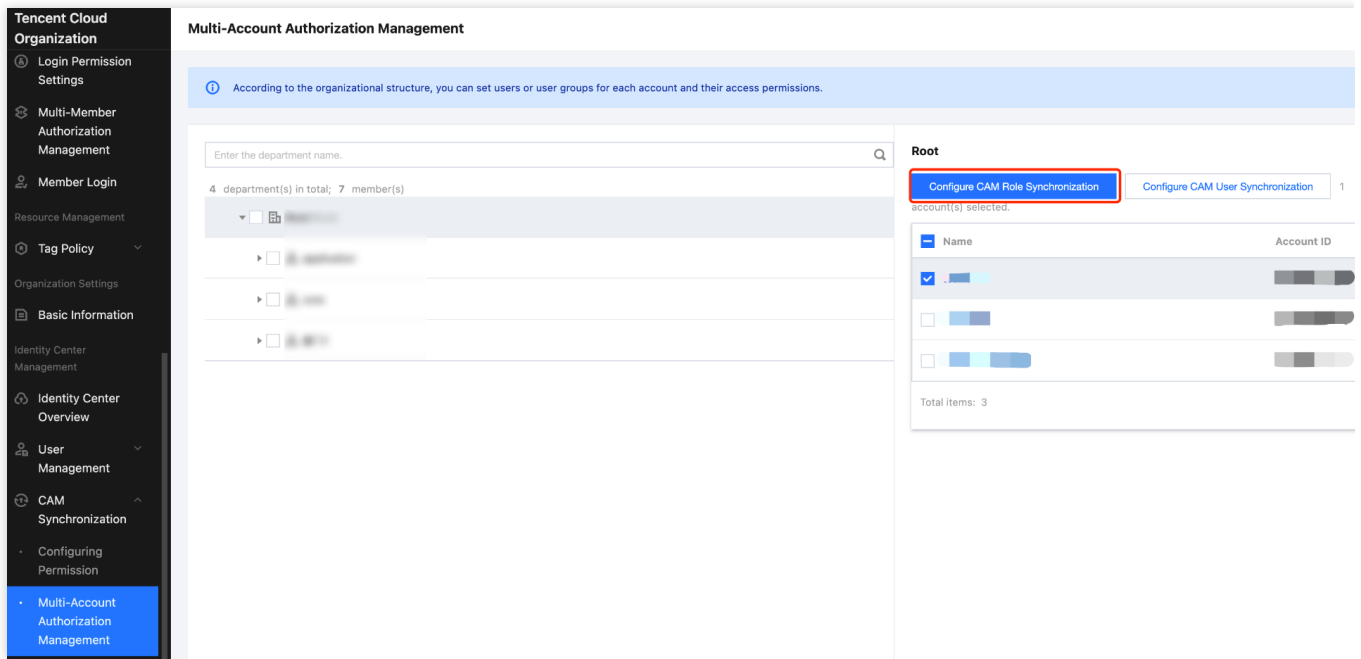
In this example, the permission configuration has been bound to preset policies, with no user-defined policies created.

Make sure you have created or synchronized a user.

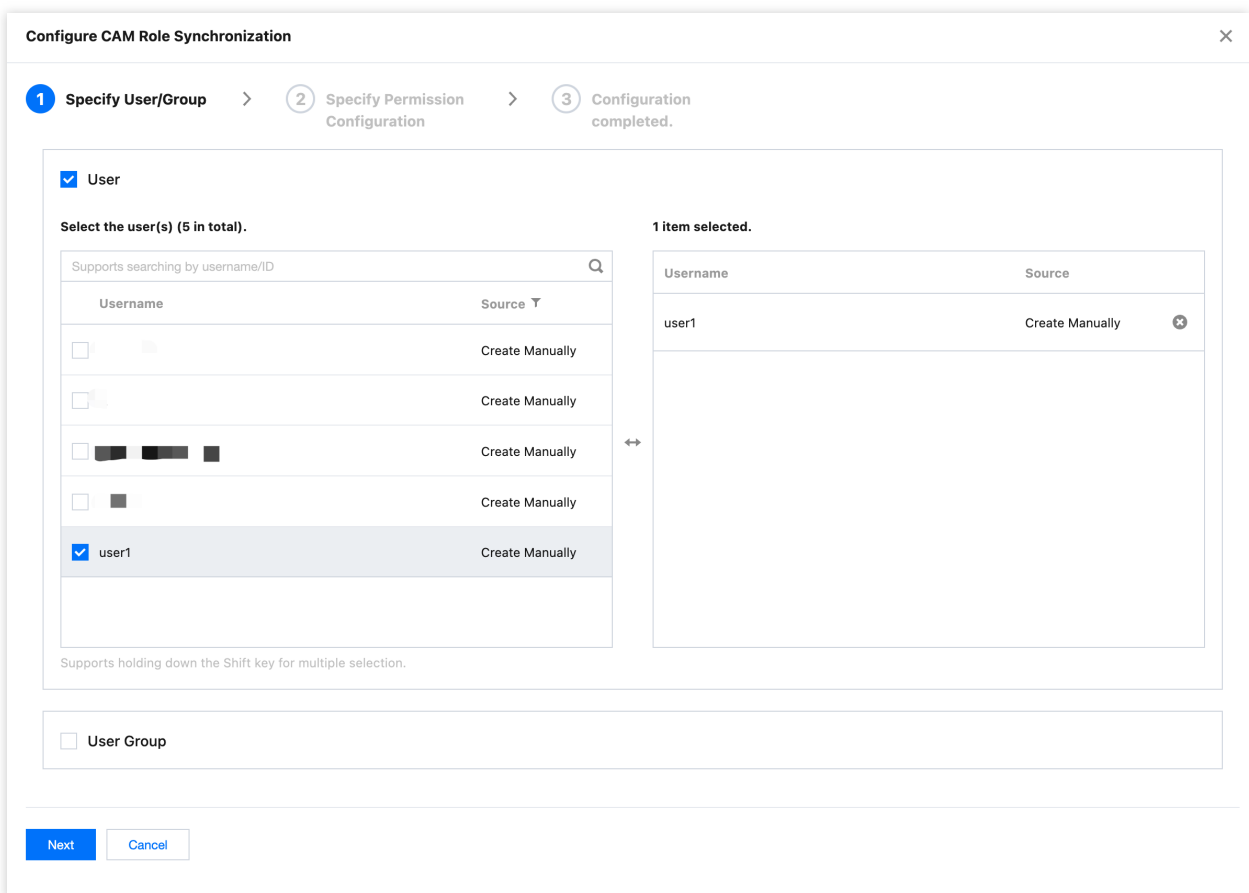
In this example, a user (user1) is created with the Identity Center. For details, refer to [Manage Users](#).

Directions

1. Go to **TCO** > [Identity Center](#).
2. In the left sidebar, click **CAM Synchronization** > **Multi-Account Authorization Management**.
3. On the **Multi-Account Authorization Management** page, select the target account.
In this example, select the member account (Account1).
4. Click **Configure CAM Role Synchronization**.



5. On the **Configure CAM Role Synchronization** page, select the target user or user group, and then click Next. In this example, select the user (user1).



6. Select the target **Permission Configuration**, and then click Next.

Configure CAM Role Synchronization

✓ Specify User/Group

 >

2 Specify Permission Configuration

 >

3 Configuration completed.

| Permission Configuration Name | Description | Creation Time |
|---|-------------|---------------------|
| <input type="checkbox"/> test2 | - | 2024-07-30 11:27:51 |
| <input type="checkbox"/> root1 | - | 2024-07-18 11:27:51 |
| <input type="checkbox"/> root | - | 2024-07-18 11:25:43 |
| <input type="checkbox"/> test | - | 2024-07-18 11:22:52 |
| <input type="checkbox"/> sec-testpolicy | - | 2024-07-18 10:55:29 |
| <input type="checkbox"/> A | - | 2024-07-16 16:24:32 |
| <input type="checkbox"/> test1 | - | 2024-07-12 14:26:13 |

0 item(s) selected, with a total of 7 item(s).

7. Review the configuration information, and then click **Submit**.

Configure CAM Role Synchronization

✓ Specify User/Group

 >

✓ Specify Permission Configuration

 >

3 Configuration completed.

Selected Account
Account Name/ID ██ ██ ██ ██ ██ ██

Selected Permission Configuration
Permission configuration selected. [test1](#)

Selected User/Group
User/Group selected. 1 users; 0 user groups
User selected.
[user1](#)

8. Wait for the configuration to finish, and then click **Completed**.

Result Verification

1. Log in to the Group Account Identity Center Portal using the Identity Center user (user1).

For detailed operations, refer to [Identity Center User Login](#).

2. On the **CAM Role Login** tab, click Show Details in the permission column of the member account (Account1).

3. On the permission panel, click **Log in** in the **Action** column of the target permission configuration.

4. Access CVM resources in the member account (Account1) as a CAM Role.

Note:

Since only access to CVM is configured, you can only access CVM Resources. If you need to access other resources, modify policies in the permission configuration and redeploy the permission configuration.

View/Modify/Delete Authorization

Last updated : 2024-07-31 14:17:23

Overview

This document introduces how to view the authorization information, modify the authorization, and delete the authorization of an account.

Directions

Viewing Authorization Information

1. Go to **TCO** > [Identity Center](#).
2. In the left sidebar, click **CAM Synchronization** > **Multi-Account Authorization Management**.
3. On the **Multi-Account Authorization Management** page, click the target account name.
4. View the authorization information of the account.

In the **Basic Information** area, view the basic information of the account.

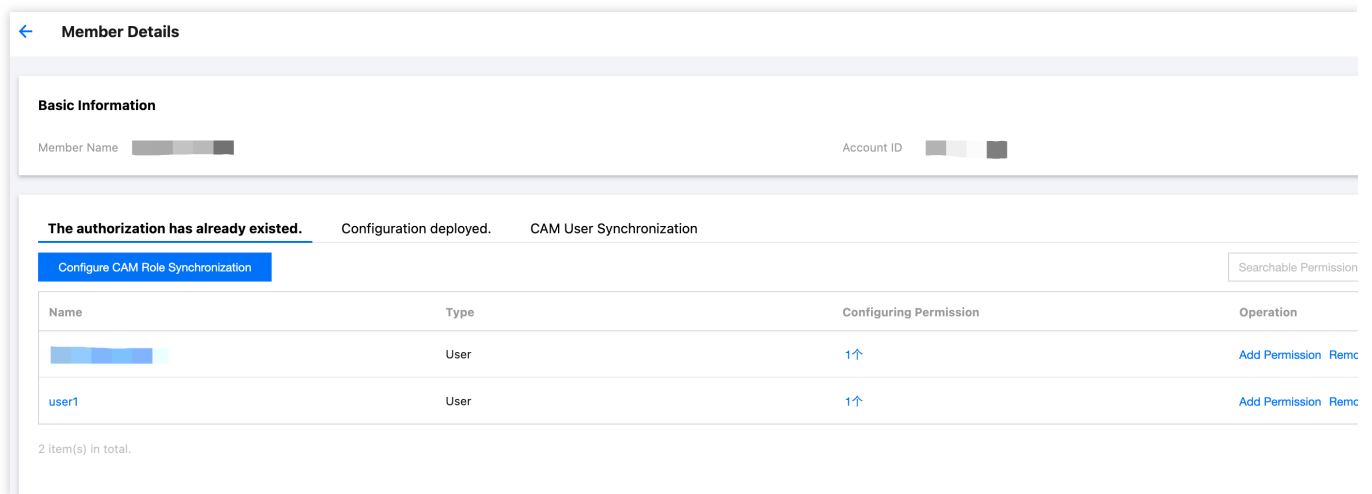
In the **The authorization has already existed** tab, view the users or user groups associated with the account.

In the **Configuration deployed** tab, view the permissions configuration deployed in the account.

In the **CAM User Synchronization** tab, view the configured CAM user synchronization information.

Modifying the Authorization

1. Go to **TCO** > [Identity Center](#).
2. In the left sidebar, click **CAM Synchronization** > **Multi-Account Authorization Management**.
3. On the **Multi-Account Authorization Management** page, click the target account name.
4. Click the **The authorization has already existed** tab
5. Click **Configure CAM Role Synchronization**.



6. On the **Configure CAM Role Synchronization** panel, reassign users, user groups, and permission configuration.

Select a user or user group, and then click **Next**.

Select permission configuration, and then click **Next**.

Review the configuration information, and then click **Start Configuration**.

Wait for the deployment to finish, and then click **Finish**.

Deleting the Authorization

1. Go to **TCO > Identity Center**.

2. In the left sidebar, click **CAM Synchronization > Multi-account Authorization Management**.

3. On the **Multi-Account Authorization Management** page, click the target account name.

4. Click the **The authorization has already existed** tab.

5. Click **Remove Permissions** in the action column of the target user or user group.

6. In the confirmation dialog box, click **OK**.

7. Click **Completed**.

Manage CAM User Synchronization

Configure CAM User Synchronization

Last updated : 2024-07-31 14:17:23

Overview

You can configure CAM user synchronization, create a CAM user in the target account with the same name as the Identity Center user, and then access resources in the account via the CAM user.

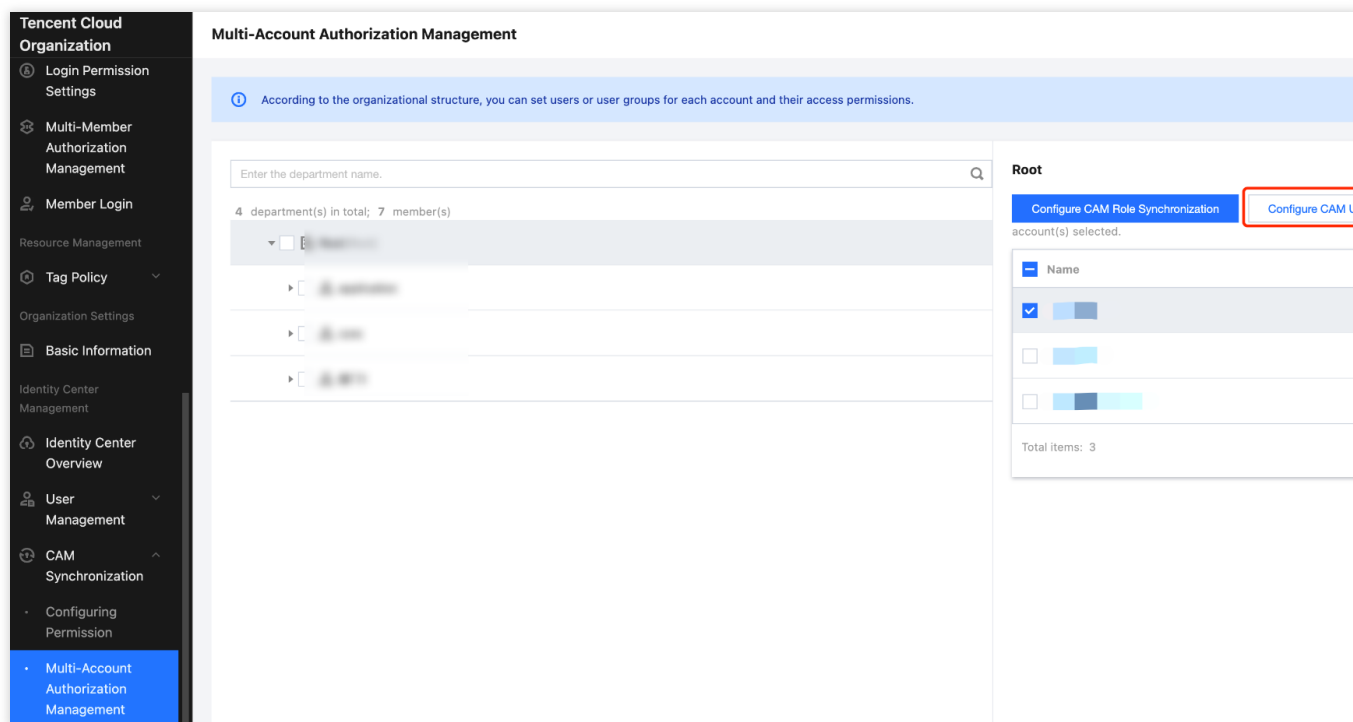
This document provides an example of how to configure CAM user synchronization, create a CAM user (user1@tencent) in the member account (Account1) with the same name as the Identity Center user (user1), and then grant administrative permissions for CVM to the CAM user (user1@tencent), enabling access to CVM resources in the member account (Account1) via the CAM user (user1@tencent).

Directions

Step 1: Configuring CAM User Synchronization

Use the administrative account to configure CAM user synchronization in the Identity Center.

1. Go to **TCO** > [Identity Center](#).
2. In the left sidebar, click **CAM Synchronization** > **Multi-Account Authorization Management**.
3. On the **Multi-Account Authorization Management** page, select the target account.
In this example, select the member account (Account1).
4. Click **Configure CAM User Synchronization**.



5. On the **Configure CAM User Synchronization** panel, select the target user or user group, and then click **Next**. In this example, select the Identity Center user (user1).

Configure CAM User Synchronization

1 Specify User/Group
2 Set Basic Information
3 Configuration completed.

☒ User

Select the user(s) (5 in total).

Supports searching by username/ID

| Username | Source |
|---|-----------------|
| <input type="checkbox"/> | Create Manually |
| <input type="checkbox"/> | Create Manually |
| <input type="checkbox"/> | Create Manually |
| <input type="checkbox"/> | Create Manually |
| <input checked="" type="checkbox"/> user1 | Create Manually |

1 item selected.

| Username | Source |
|----------|-----------------|
| user1 | Create Manually |

☐ User Group

Next Cancel

6. Configure the following basic information, and then click **Next**.

6.1 Enter a description of CAM user synchronization.

6.2 Configure **Conflicting Policy**.

Conflicting Policy: the handling policy when a CAM user with the same name exists in the target account.

Replace: The newly created CAM user will overwrite the existing CAM user.

Save Both: The newly created CAM user will be renamed by the system, and both the new and old CAM users will be retained.

6.3 Configure **Delete Policy**.

Delete Policy: the handling policy for already synchronized CAM users when CAM user synchronization is deleted.

Save: When CAM user synchronization is deleted, the already synchronized CAM user will be retained.

Delete: When CAM user synchronization is deleted, the already synchronized CAM user will be deleted.

Configure CAM User Synchronization

✓ Specify User/Group

>

2 Set Basic Information

>

3 Configuration completed.

CAM User Synchronization Configuration

Description

Enter the description information.

Processing Mode

Batch Operations

Conflicting Policy *

Replace

The newly created CAM user will override the existing CAM user.

Delete Policy *

Save

When the CAM user synchronization is deleted in the identity center, the synchronized user in the CAM will be retained.

Users/Groups to Be Synchronized

User/Group selected.

1 users; 0 user groups

User selected.

user1

Back

Next

Cancel

7. Click **Completed**.

After successful configuration, a CAM user with the same name will be created in the target account. In this example, a CAM user (user1@tencent) with the same name as the Identity Center user (user1) will be synchronously created in the member account (Account1).

Step 2: Authorizing the CAM User

Through [Identity Center](#) > **Configure CAM User Synchronization**, the synchronized sub-user in CAM is not granted any permissions. You need to authorize the user on the CAM console. If you need to preset permissions through the Identity Center, choose to configure CAM role synchronization.

1. Log in to the member account (Account1).
2. Authorize the CAM user (user1@tencent).

In this example, the CAM user (user1@tencent) will be granted administrative permissions for CVM. For specific operations, refer to [Sub-user Permission Settings](#).

Step 3: The Identity Center User Accesses Tencent Cloud

The Identity Center user (user1) accesses CVM resources in the member account (Account1) via the CAM user (user1@tencent).

1. The Identity Center user (user1) logs in to the Identity Center User Portal.

For detailed operations, refer to [Identity Center User Login](#).

2. Access CVM resources in the member account (Account1) as a CAM user.

View/Modify/Delete User Synchronization

Last updated : 2024-07-31 14:17:23

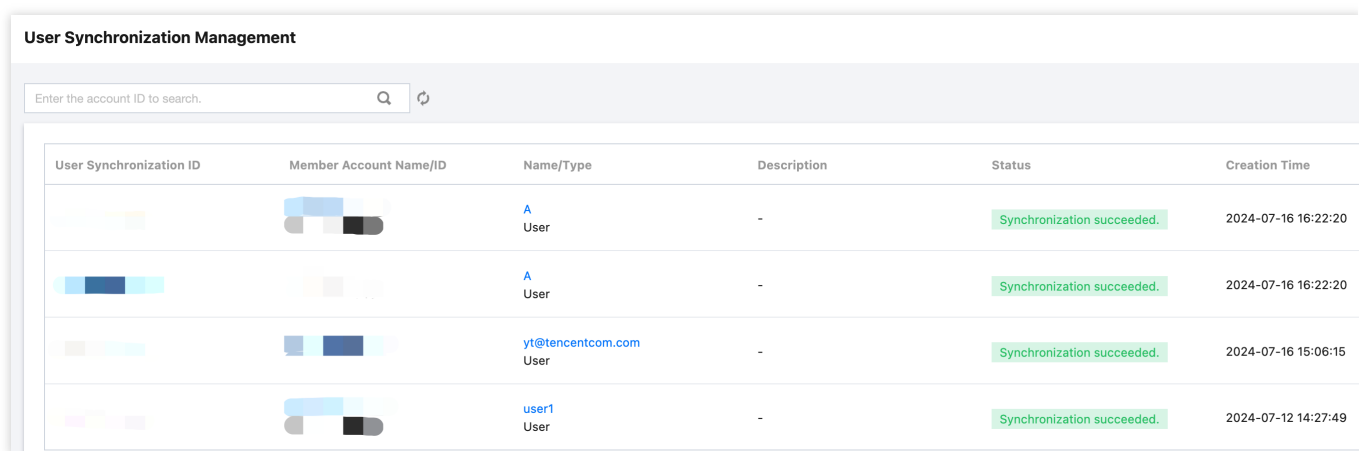
Overview

This document introduces how to view CAM user synchronization details, modify CAM user synchronization, and delete CAM user synchronization.

Directions

Viewing CAM User Synchronization

1. Go to **TCO** > [Identity Center](#).
2. In the left sidebar, select **CAM Synchronization** > **User Synchronization Management**.



The screenshot displays the 'User Synchronization Management' interface. At the top, there is a search bar with the placeholder text 'Enter the account ID to search.' and a refresh icon. Below the search bar is a table with the following columns: 'User Synchronization ID', 'Member Account Name/ID', 'Name/Type', 'Description', 'Status', and 'Creation Time'. The table contains four rows of data, each representing a user synchronization record. The first three rows show 'Synchronization succeeded.' status, and the fourth row shows 'Synchronization succeeded.' status. The 'Creation Time' for the first three rows is '2024-07-16 16:22:20', and for the fourth row, it is '2024-07-12 14:27:49'.

| User Synchronization ID | Member Account Name/ID | Name/Type | Description | Status | Creation Time |
|-------------------------|------------------------|---------------------------|-------------|----------------------------|---------------------|
| | | A User | - | Synchronization succeeded. | 2024-07-16 16:22:20 |
| | | A User | - | Synchronization succeeded. | 2024-07-16 16:22:20 |
| | | yt@tencentcom.com User | - | Synchronization succeeded. | 2024-07-16 15:06:15 |
| | | user1 User | - | Synchronization succeeded. | 2024-07-12 14:27:49 |

3. On the **User Synchronization Management** page, click the **Operation** column of the target user synchronization and select **View Details**.
4. On the **User Synchronization Details** panel, view the user synchronization details, including CAM user synchronization ID, status, deletion policy, conflict policy, and creation time.

Modifying CAM User Synchronization

1. Go to **TCO** > [Identity Center](#).
2. In the left sidebar, select **CAM Synchronization** > **User Synchronization Management**.
3. On the **User Synchronization Management** page, click the **Operation** column of the target user synchronization and select **View Details**.

4. On the **User Synchronization Details** panel, click **Edit** to modify the description or deletion policy.
- For the meaning of configuration items, see [Configure CAM User Synchronization](#).

| User Synchronization Management | | | | | CAM User Synchroniz |
|---------------------------------|------------------------|---------------------------|-------------|----------------------------|--------------------------|
| Enter the account ID to search. | | | | | CAM User Synchronization |
| User Synchronization ID | Member Account Name/ID | Name/Type | Description | Status | Status |
| | | A User | - | Synchronization succeeded. | Description |
| | | A User | - | Synchronization succeeded. | Delete Policy |
| | | yt@tencentcom.com User | - | Synchronization succeeded. | Conflicting Policy |
| | | user1 User | - | Synchronization succeeded. | Account ID |
| | | | | | Identity Type |
| | | | | | Creation Time |
| | | | | | Update Time |

Deleting CAM User Synchronization

1. Go to **TCO > Identity Center**.
2. In the left sidebar, select **CAM Synchronization > User Synchronization Management**.
3. On the **User Synchronization Management** page, click **Delete** in the **Action** column of the target user synchronization.
4. In the pop-up dialog box, click **OK**.

预览版本

Console

Search

Supports searching for resources by instance ID

Shortcut /

Organization

Tools

Settings

User Synchronization Management

Enter the account ID to search.

Search

Refresh

| User Synchronization ID | Member Account Name/ID | Name/Type | Description | Status | Creation Time |
|--|------------------------|-----------|-------------|--------|---------------|
| 1234567890 | | | | | |

Identity Center User Login

Last updated : 2024-07-31 14:17:23

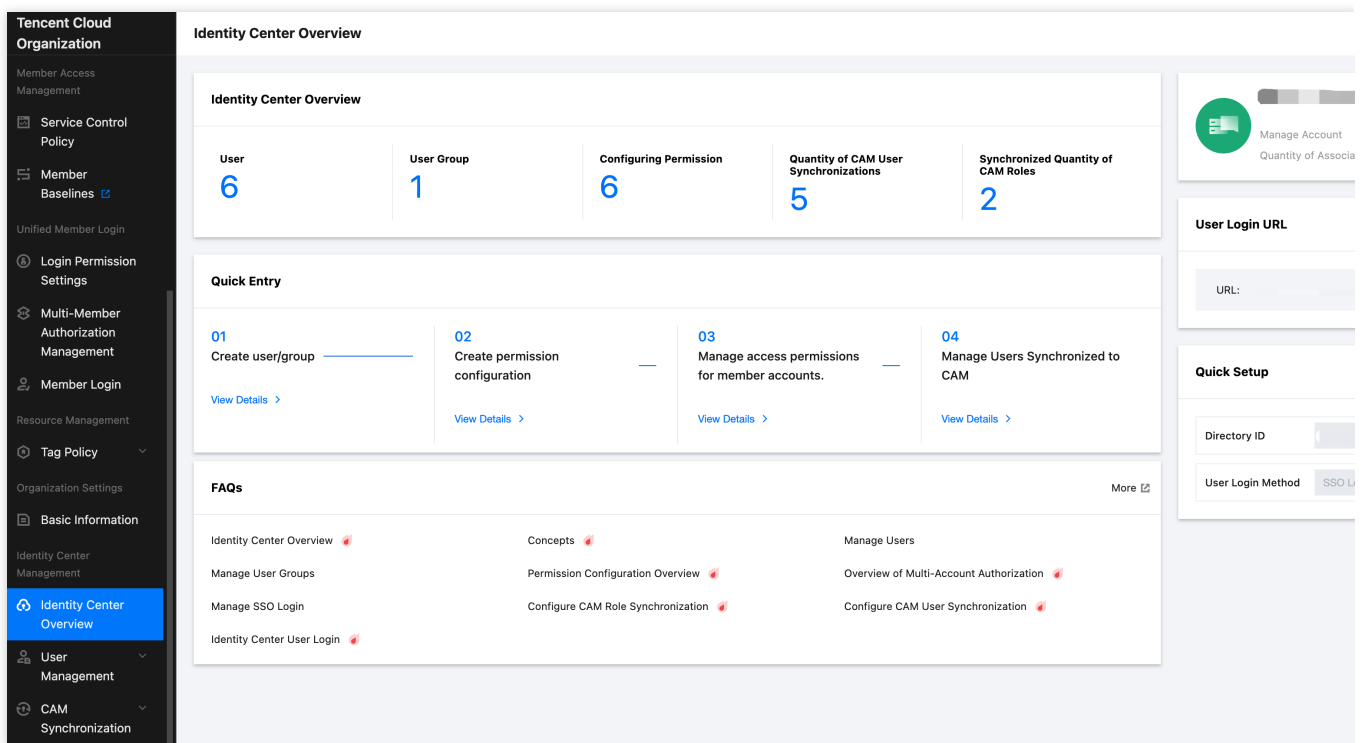
Overview

When Identity Center users log in to the user portal, they can view accounts they have permissions to access and access corresponding resources as CAM roles or CAM users.

Directions

Step 1: Obtain the Login Portal URL

1. The Identity Center administrator goes to **TCO** > [Identity Center](#).
2. On the left sidebar, click **Identity Center Overview**.
3. On the right side of the overview page, view or copy **User Login URL**.



Step 2: Log In to the Identity Center User Portal

1. Identity Center users click to access **User Login URL**.

2. Log in to the Identity Center user portal according to the configured login method.

Note:

Single sign-on (SSO) is supported for users, while password login is not supported currently.

3. On the SSO login page, click **Redirect**, and the system will automatically redirect to the enterprise IdP login page.

4. Log in with your enterprise IdP username and password.

Step 3: Access Accounts

Log In with a CAM Role

For cloud services that support CAM roles and have access permissions configured in the Identity Center, you can access account resources using a CAM role. This method applies to most cloud services. For configuration methods, refer to [Configuring CAM Role Synchronization](#).

1. On the **Log In with a CAM Role** tab, click the **Permission Details** in the **Permissions** column of the target account. When you have access to multiple accounts, you can flexibly choose the account you want to access on this page.

Note:

If the list is empty, it means you do not have access to any accounts.

2. Click **Log In** in the **Operation** column of the target permission. When you have multiple permissions on the target account, you can flexibly choose the permission you want to use on this page.

Log In with a CAM User

For cloud services that do not support CAM roles and have CAM user synchronization configured in the Identity Center, you can access account resources as a CAM user. For configuration methods, refer to [Configuring CAM User Synchronization](#).

1. On the Log In with a CAM User tab, click **Log In** in the **Operation** column of the target account. When you have access to multiple accounts, you can flexibly choose the account you want to access on this page.

Note:

If the list is empty, it means you do not have access to any accounts.