Cloud Organization

Product Documentation

Contents

Cloud Organization 4
- Product Introduction 4
  - Product Introduction 4
  - Relevant Concepts 5
- Operation Guide 7
  - Group Organization Settings 7
    - Creating a Group Organization 7
    - Viewing Group Organization Information 8
    - Viewing of Invitation Information by Users 9
    - Acceptance or Rejection of Invitations by Users 10
    - Member Withdrawal from the Group Organization 11
  - Group Organization Information Overview 12
    - Organization Finance Overview 12
  - Department Management 13
    - Creating a Department 13
    - Modifying Department Information 15
    - Deleting a Department 17
    - Moving Members 18
  - Member Account Management 21
    - Viewing or Editing Basic Member Information 21
    - Removing Organization Members 23
    - Adding an Organization Member 24
    - Canceling a Member Invitation 25
    - Creating Member Login Permissions 26
    - Configuring Login Permissions for Members 28
    - Authorizing Member Account Login 31
  - Member Financial Management 37
    - Organization Finance Overview 37
  - Identity Center Management 39
    - Introduction to Identity Center 39
      - Introduction to Identity Center 39
      - Basic Concepts 41
    - Identity Center Use Cases 43
      - Logging In with a Cloud Platform Sub-account 43
    - Enabling a Service 48
    - Managing Users 49
    - Managing User Groups 52
    - Settings 55
      - SCIM synchronization 55
        - Managing SCIM Keys 55
        - Enabling or Disabling SCIM Synchronization 59
        - SCIM Synchronization Example 61
          - Examples of Synchronization from Azure AD via SCIM 61
        - SCIM 2.0 APIs 65
      - Managing SSO 87
    - Managing Multi-Account Authorization 91
      - Multi-account Authorization Overview 91
      - Configuring CAM Role Synchronization 93
    - Managing CAM User Synchronization 94
      - Configuring CAM User Synchronization 94
      - Viewing/Modifying/Deleting User Synchronization 97
    - User Login 99
      - Identity Center User Login 99
- FAQs 101
  - Operation FAQs 101
- API Documentation 103
  - Cam Identity Center(cic) 103
    - version(2021-03-31) 103
      - API overview 103
      - CallingMethod 107
        - signaturev1 107
        - signaturev3 115
        - request 124
        - result 125
        - PublicParameter 128
      - Identity Center Management APIs 130
        - DescribeIdentityCenter 130
        - GetZoneStatistics 131
        - OpenIdentityCenter 133
        - UpdateZone 134
      - Identity Center Management SCIM Synchronization APIs 135
        - CreateSCIMCredential 135
        - DeleteSCIMCredential 137
        - GetSCIMSynchronizationStatus 139
        - ListSCIMCredentials 141
        - UpdateSCIMCredentialStatus 143
        - UpdateSCIMSynchronizationStatus 145
      - Identity Center Multi-Account Authorization Management APIs 147
        - CreateRoleAssignment 147
      - Identity Center Permission Configuration Management APIs 149
        - CreateRoleConfiguration 149
      - Identity Center Single Sign-On Management APIs 150
        - AddExternalSAMLIdPCertificate 150
        - ClearExternalSAMLIdentityProvider 152
        - GetExternalSAMLIdentityProvider 154
        - GetZoneDetail 156
        - GetZoneSAMLServiceProviderInfo 157
        - ListExternalSAMLIdPCertificates 159
        - RemoveExternalSAMLIdPCertificate 161

- SetExternalSAMLIdentityProvider ... 163
- Identity Center Sub-User Synchronization Management APIs ... 165
  - CreateUserSyncProvisioning ... 165
  - DeleteUserSyncProvisioning ... 167
  - GetProvisioningTaskStatus ... 169
  - GetUserSyncProvisioning ... 171
  - ListUserSyncProvisionings ... 173
  - UpdateUserSyncProvisioning ... 174
- Identity Center User Group Management APIs ... 175
  - AddUserToGroup ... 175
  - CreateGroup ... 177
  - DeleteGroup ... 178
  - GetGroup ... 180
  - ListGroupMembers ... 182
  - ListGroups ... 183
  - ListJoinedGroupsForUser ... 184
  - RemoveUserFromGroup ... 185
  - UpdateGroup ... 187
- Identity Center User Management APIs ... 189
  - CreateUser ... 189
  - DeleteUser ... 190
  - GetUser ... 192
  - ListUsers ... 194
  - UpdateUser ... 195
  - UpdateUserStatus ... 197
- Data structure ... 199
- ErrorCode ... 202

- Organization Account Management(organization) ... 209
  - version(2022-05-08) ... 209
    - API overview ... 209
    - CallingMethod ... 212
      - signaturev1 ... 212
      - signaturev3 ... 220
      - request ... 229
      - result ... 230
      - PublicParameter ... 233
    - Department and Member Management APIs ... 235
      - AddOrganizationMemberEmail ... 235
      - CheckAccountDelete ... 238
      - CreateOrganizationMember ... 240
      - DeleteAccount ... 242
      - DeleteOrganizationMembers ... 244
      - DescribeOrganizationMemberEmailBind ... 246
      - SendOrgMemberAccountBindEmail ... 249
      - UpdateOrganizationMember ... 251
      - UpdateOrganizationMemberEmailBind ... 252
    - Financial Overview APIs ... 254
      - DescribeOrganizationFinancialByMember ... 254
      - DescribeOrganizationFinancialByMonth ... 256
      - DescribeOrganizationFinancialByProduct ... 258
    - Organization Management Policy APIs ... 260
      - ListPolicies ... 260
      - ListPoliciesForTarget ... 262
    - Organization Settings APIs ... 264
      - CreateOrganization ... 264
      - DeleteOrganization ... 266
      - QuitOrganization ... 268
    - Unified Member Login APIs ... 270
      - CreateOrganizationIdentity ... 270
      - CreateOrganizationMemberAuthIdentity ... 272
      - CreateOrganizationMembersPolicy ... 274
      - DeleteOrganizationIdentity ... 276
      - DeleteOrganizationMemberAuthIdentity ... 278
      - DeleteOrganizationMembersPolicy ... 280
      - DescribeOrganizationMemberAuthIdentities ... 282
      - DescribeOrganizationMemberPolicies ... 283
      - ListOrganizationIdentity ... 285
      - UpdateOrganizationIdentity ... 287
    - Data structure ... 289
    - ErrorCode ... 302

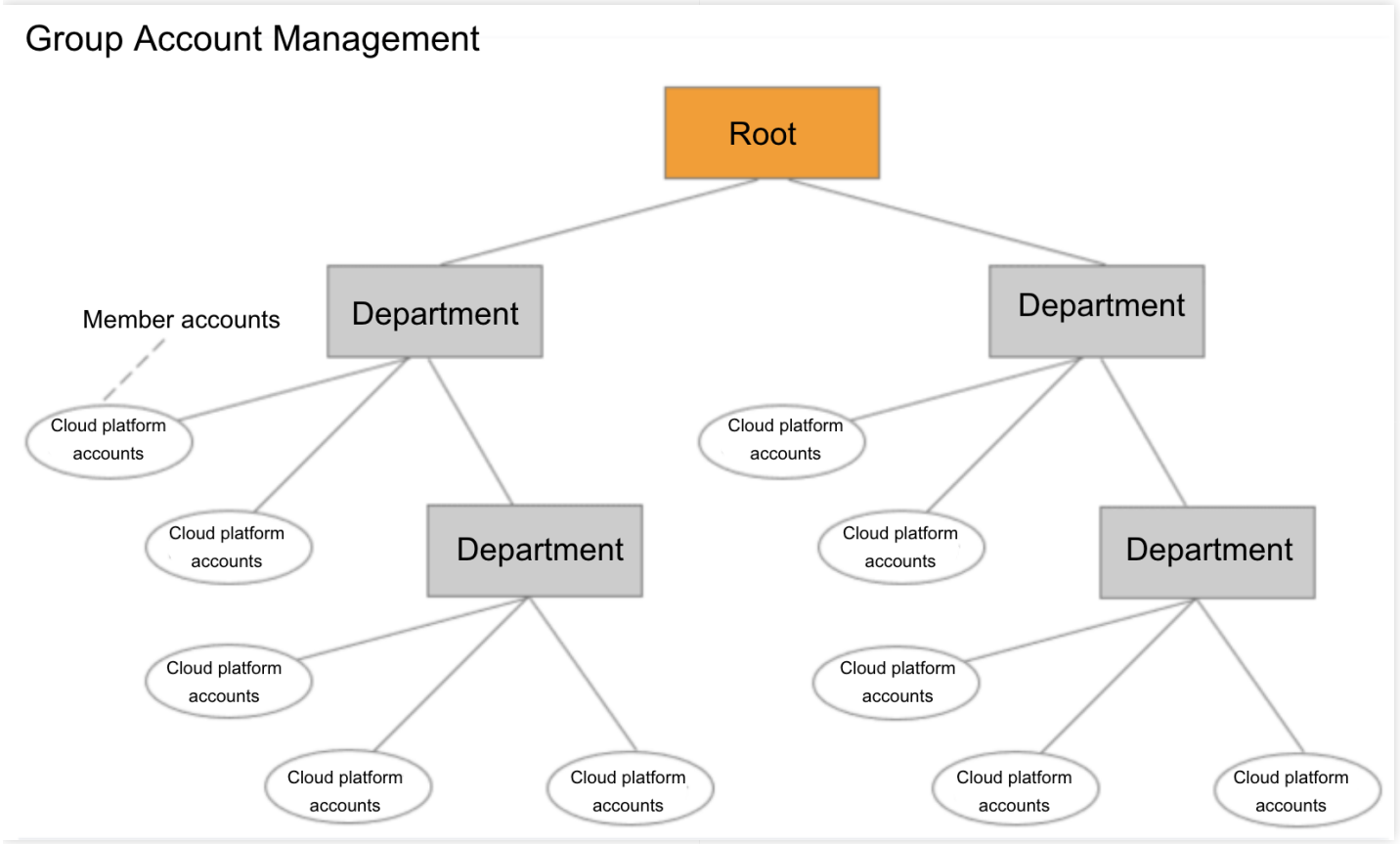
Product Introduction

Product Introduction

Cloud Organization is a multi-account management service. You can use this service to create an organization and add your own cloud account and the cloud accounts of your subsidiaries to the organization through invitation or account creation for unified management. Organization administrative accounts can log in to the console of members to manage member accounts within the permission scope. Such accounts can uniformly view and manage the consumption of all accounts of the corresponding enterprise, improving financial management efficiency.

Relevant Concepts

This document introduces the main concepts of Cloud Organization. You can quickly obtain relevant information through the following content.
The following figure illustrates a basic cloud organization containing 10 accounts, which are grouped into four departments under the root. You can refer to the following content of this document to understand the items in the figure.



Root

A root is the parent container of all accounts in an organization.

Organization

You can create organizations to sort out the hierarchical relationships between cloud accounts. You can centrally view and manage all accounts in your organization in the Cloud Organization console. An organization has one admin account and multiple member accounts. You can organize these accounts in a hierarchical tree structure, with the root at the tree top and departments nested under the root node. Each account can be placed directly under the root node or in a department of the hierarchy.

Department

A department is a node used to store accounts under the root node and can contain other departments. This enables you to create a hierarchy similar to a reverse tree with the root node at the top, departments extending downward, and accounts at the bottom.

Account

An account is a standard cloud account that contains your cloud resources.

- Admin account: The creator of an organization is the organization's admin account. One organization can have only one admin account.
- Member account: Member accounts are other accounts than the admin account in an organization. The organization administrator can create accounts or invite other existing accounts to join the organization, remove accounts from the organization, manage invitations, and apply policies to entities like the root, departments, or accounts in the organization. One account can join only one organization.

Organization Invitation

Invitation is the process of inviting another account to join your organization. An invitation can be sent only by the root account and can be extended to account IDs associated with the invitee account. After the invitee account accepts the invitation, it will become a member account in the organization.

Operation Guide
Group Organization Settings
Creating a Group Organization

Contact the operation-side administrator for assistance in creating a group organization and adding members to the organization.

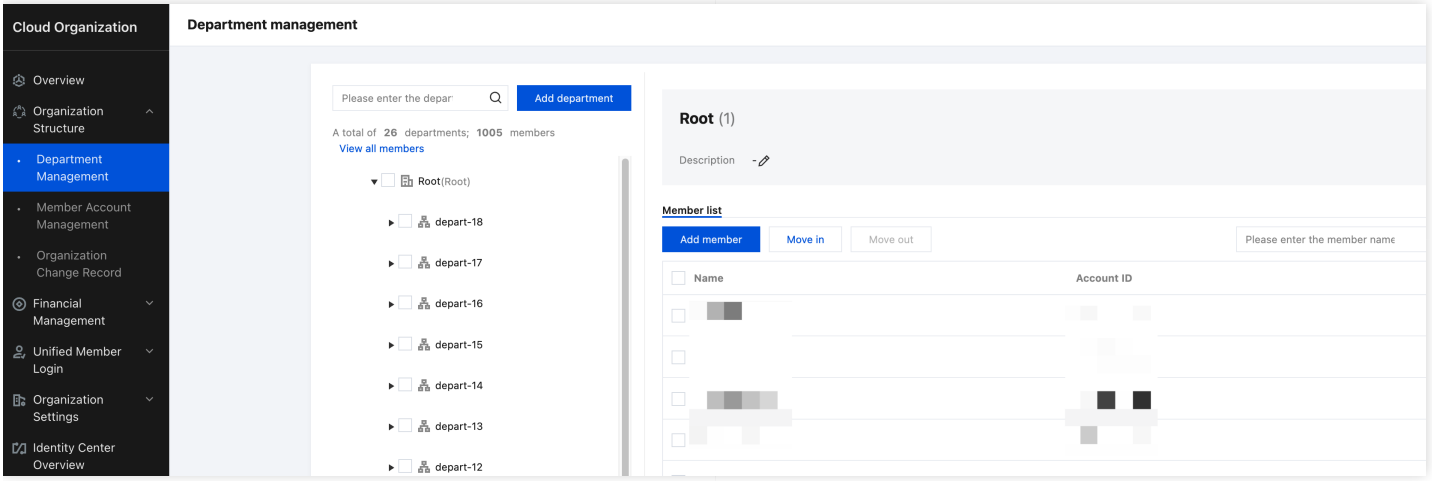
Viewing Group Organization Information

Scenarios

The group administrator or members can view organization department information in Cloud Organization.

Operation Steps

Log in to the Cloud Organization console. In the left sidebar, click Department Management to view organization information, including the department name, member name, and member ID.

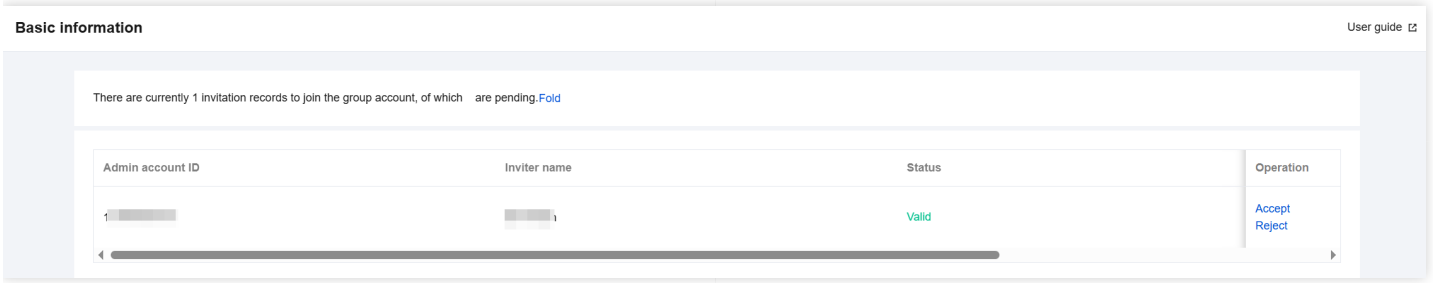


Viewing of Invitation Information by Users

Users can view the invitation message from the organization in the Cloud Organization console.

Operation Steps

Log in to the Cloud Organization console. In the left sidebar, choose Group Settings > Basic Information to view records, as shown in the following figure:



> Note
>
> - When you are not a member of any organization, you can view the invitation information.
> - The invitation list only shows the invitation records in the last three months.
> - An invitation record is valid for up to 15 days.

Acceptance or Rejection of Invitations by Users

Users can accept or reject group organization invitations in the Cloud Organization console.

Operation Steps

Log in to the Cloud Organization console. In the left sidebar, choose Group Settings > Basic Information to view the invitation records within the validity period on the Basic Information page. Click Accept to join the organization.
To reject joining the organization, click Reject, as shown in the following figure:

> Note
>
> - After you join the organization, the invitation list will be hidden until you withdraw from the organization.

Member Withdrawal from the Group Organization

If the admin account enables members to voluntarily withdraw from a group organization, they can withdraw from the organization they joined.

Operation Steps

1. Log in to the Cloud Organization console with a member account. In the left sidebar, choose Group Settings > Basic Information.

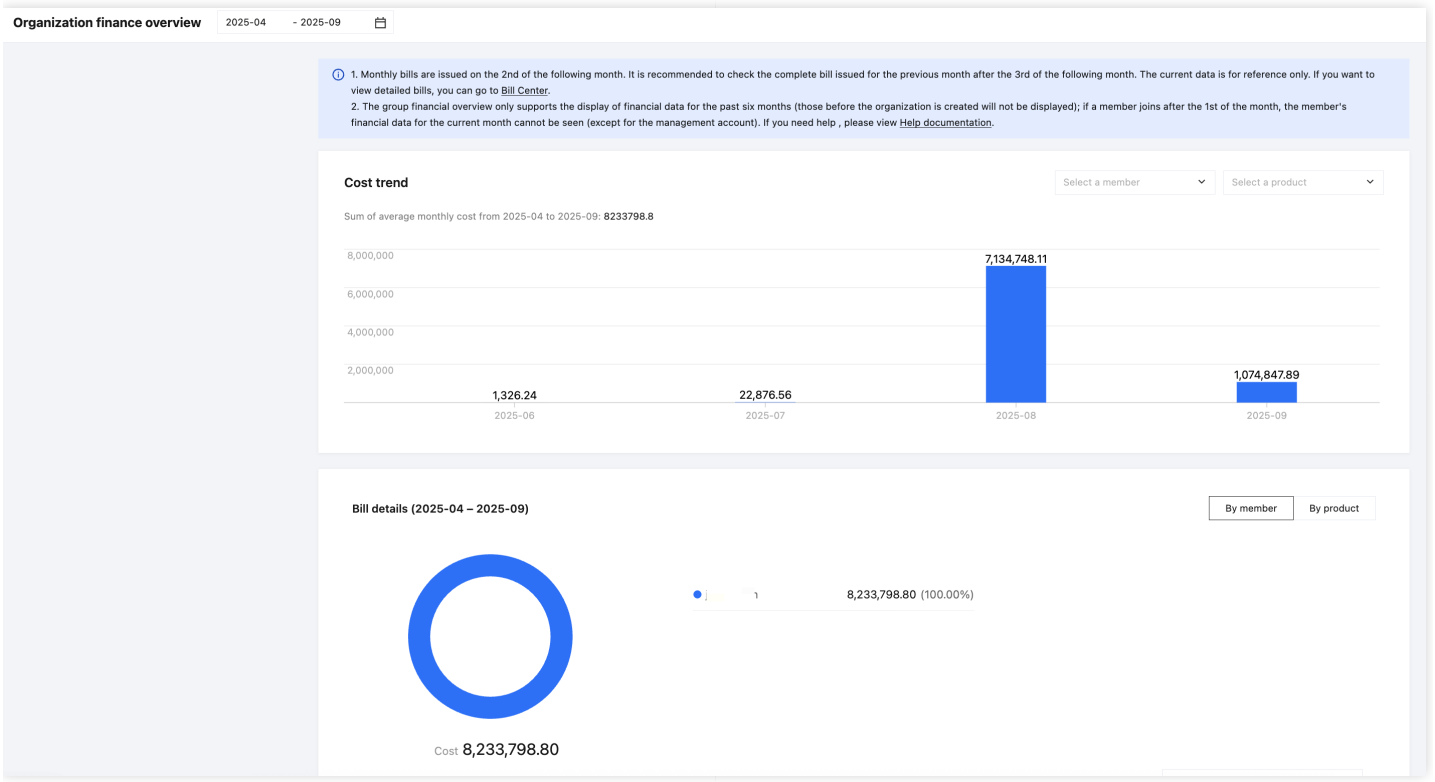
2. On the Basic Information page, click Leave Organization, as shown in the figure below:

3. In the pop-up Delete Cloud Organization confirmation window, click Confirm to withdraw from the organization.

   > Note:
   >
   > In the following scenarios, a member cannot directly withdraw from its organization:
   >
   > - The group administrator does not allow the member to withdraw from the organization through settings.
   >   The member needs to first communicate with the administrator, and the administrator allows the member to voluntarily withdraw from the organization through settings, or the admin account removes the member from the organization.

Group Organization Information Overview Organization Finance Overview

Organization Finance Overview offers a historical financial data summary of all accounts in a group organization, and supports data aggregation and viewing by dimensions such as member account and product, as shown in the following figure:



Statistics Description

- Group bill overview is provided one day after the transaction date, known as T+1. It is recommended to view the group bill overview for the current month after 15:00.
- A monthly group bill is issued on the 2nd day of the next month. It is recommended to view the complete bill issued for the previous month after 19:00.
- If a member joins the group after the 1st day of the current month, the financial data of that member for the current month is not visible (except for the admin account).

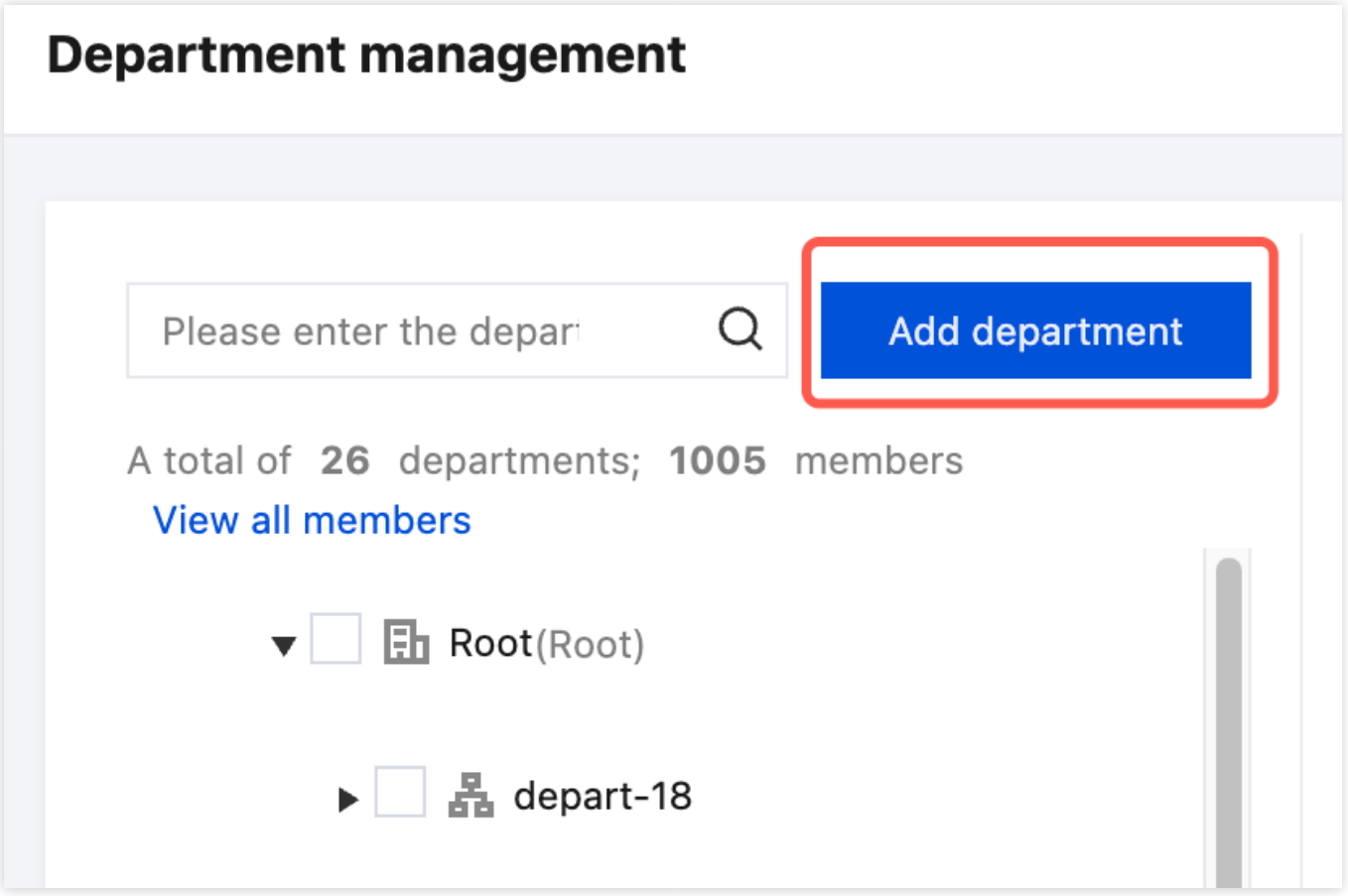
Department Management
Creating a Department

The group organization creator can manage members by department. This document introduces how to create a department in the Cloud Organization console.

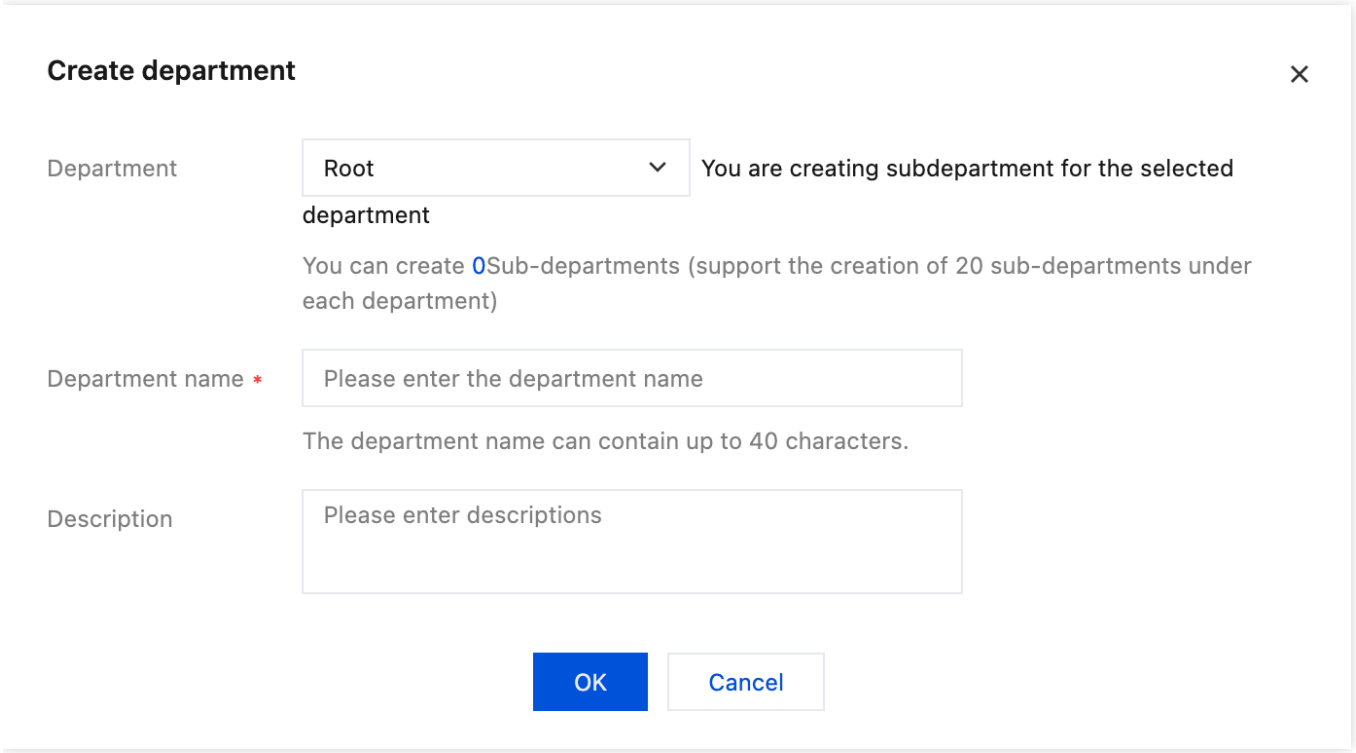
> Note
>
> An organization can contain up to five levels of department relationships.

Operation Steps

1. Log in to the Cloud Organization console. In the left sidebar, select Department Management.
2. On the Organization Structure page, click Add department, as shown in the figure below:



3. In the pop-up Create department dialog box, select a root department name, fill in a department name, enter the description, and select a tag.



4. Click OK to create a sub-department under the designated unit.

Modifying Department Information

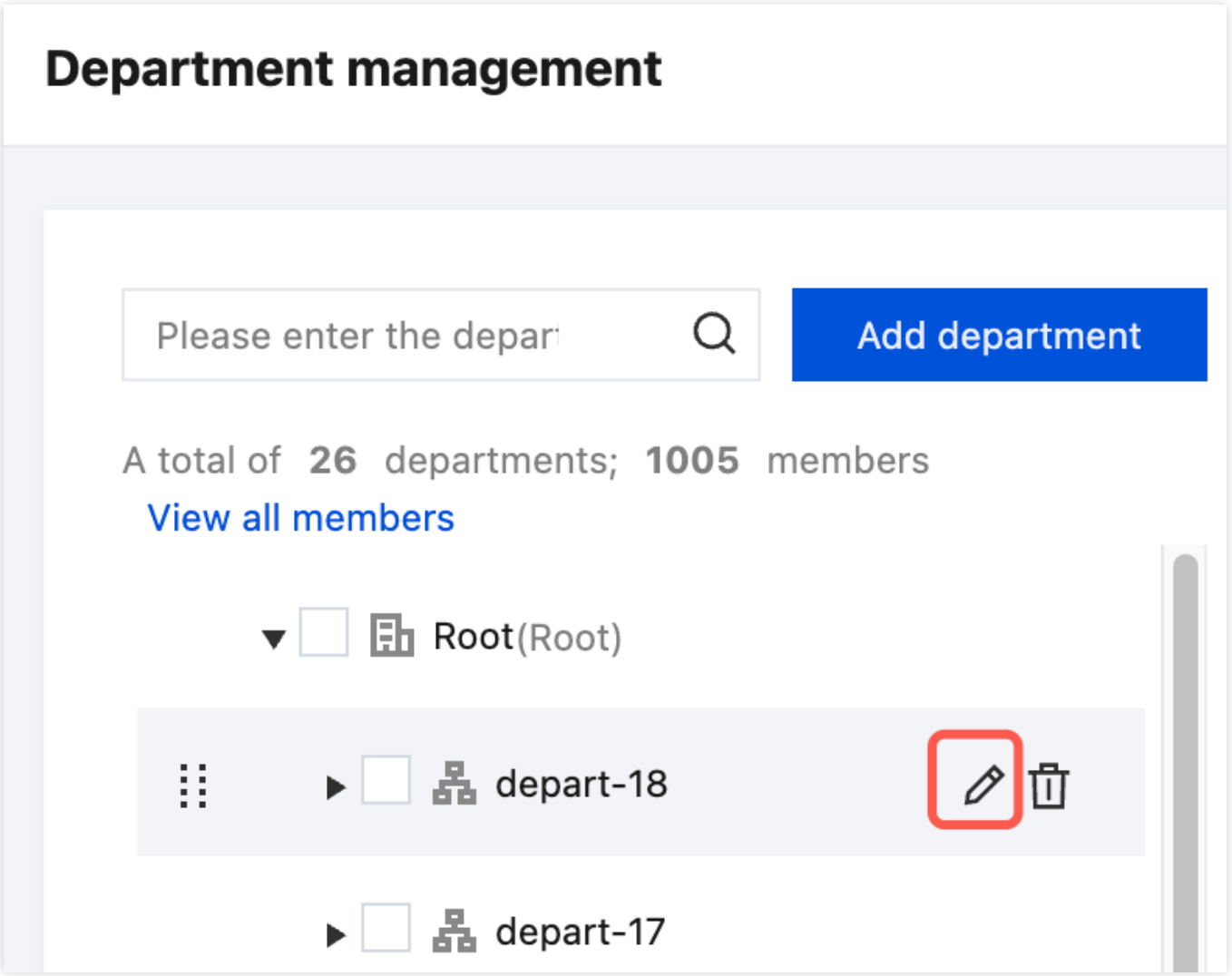
This document introduces how to modify department information in the Cloud Organization console.

Operation Steps

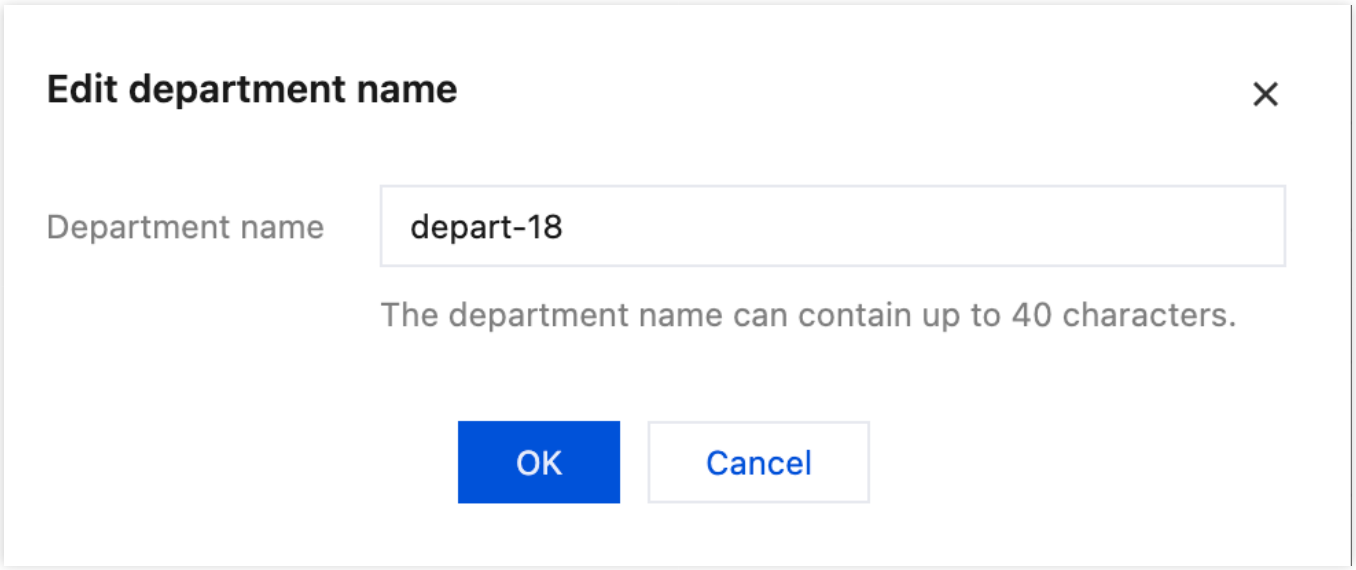
Log in to the Cloud Organization console, select Department Management in the left sidebar, and modify department-related information as needed.

Modifying the Name of a Department

1. On the Organization Structure page, hover the mouse pointer over the department to be deleted and click the on the right, as shown in the figure below:

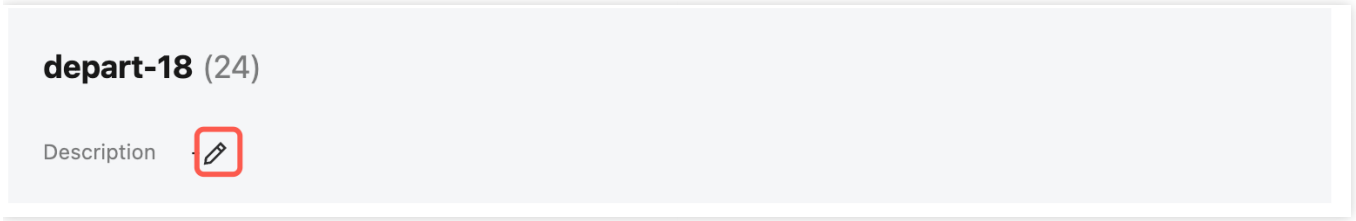


2. In the pop-up Edit department name dialog box, enter the name of the new department and click OK to complete the modification, as shown in the figure below:



Modifying the Description of a Department

In the right window of the Organization Structure page, click on the right side of Description. In the pop-up window, edit information, and click OK to complete the modification, as shown in the following figure:

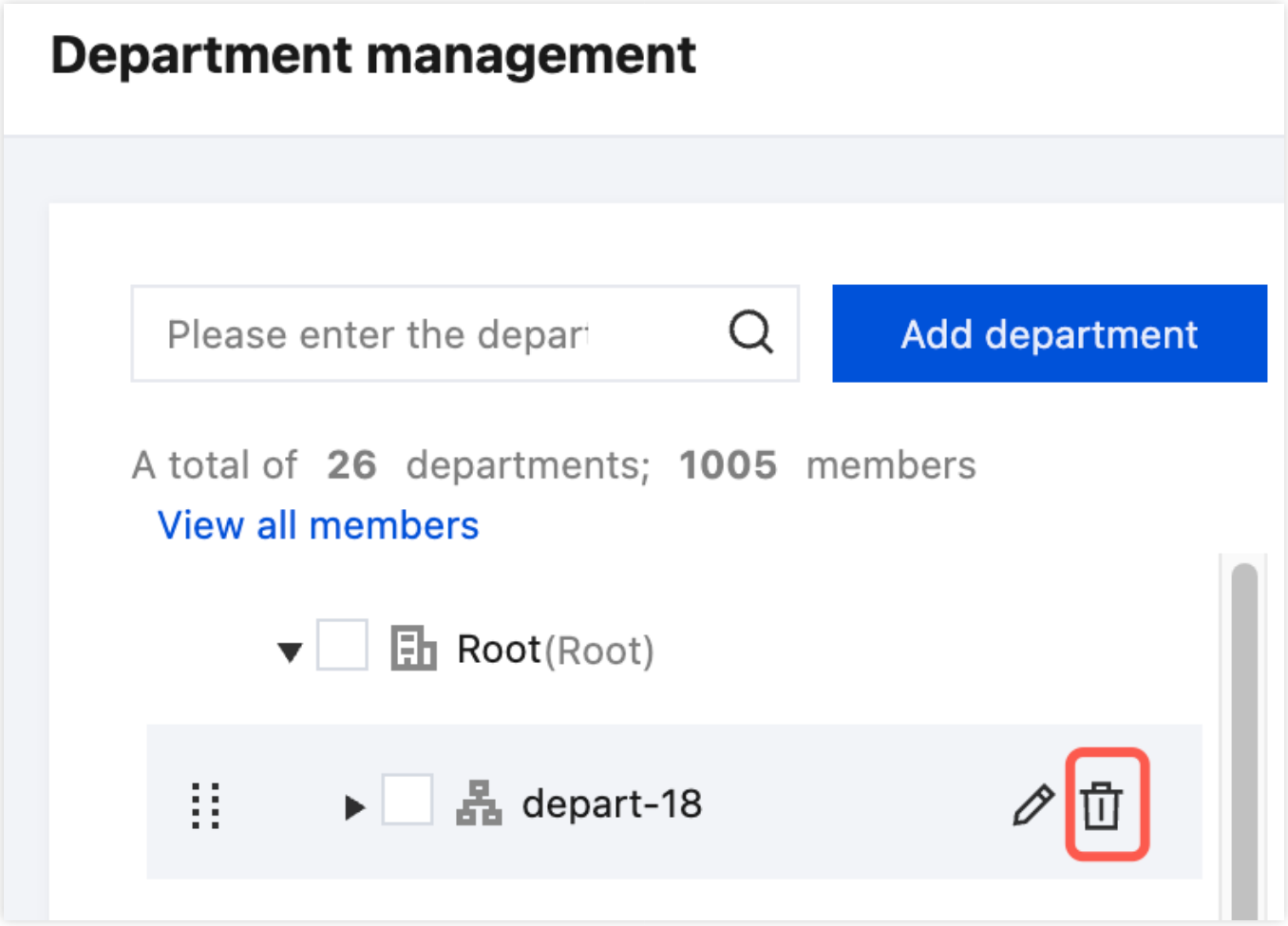


Deleting a Department

When a department is not needed, you can delete it in the Cloud Organization console.

Operation Steps

1. Log in to the Cloud Organization console. In the left sidebar, select Department Management.
2. On the Department Management page, hover the mouse pointer over the department to be deleted and click the deletion icon on the right, as shown in the figure below:



3. In the pop-up Delete department dialogbox, click Delete.

Moving Members

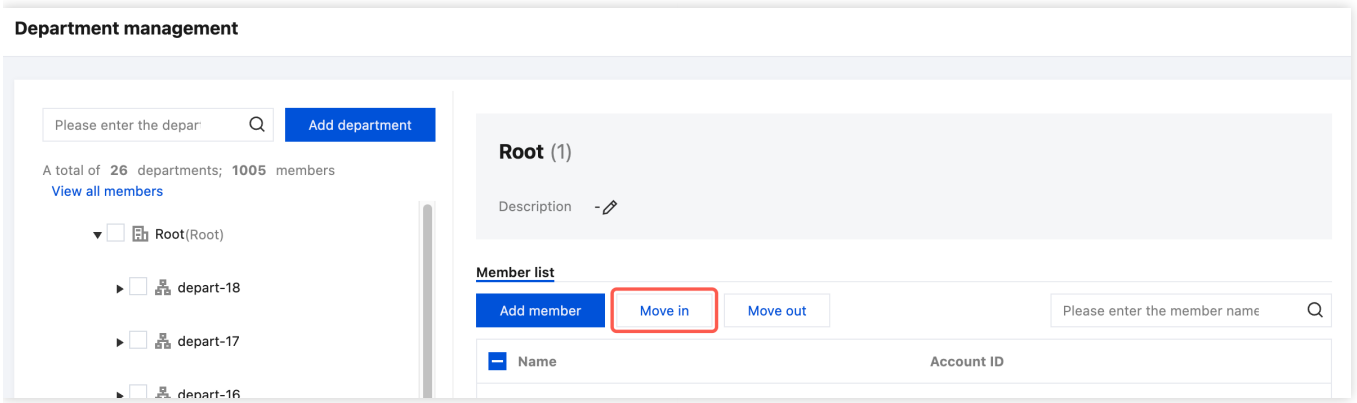
New members are placed in the root directory by default. The group organization creator can move members to the corresponding departments.

Operation Steps

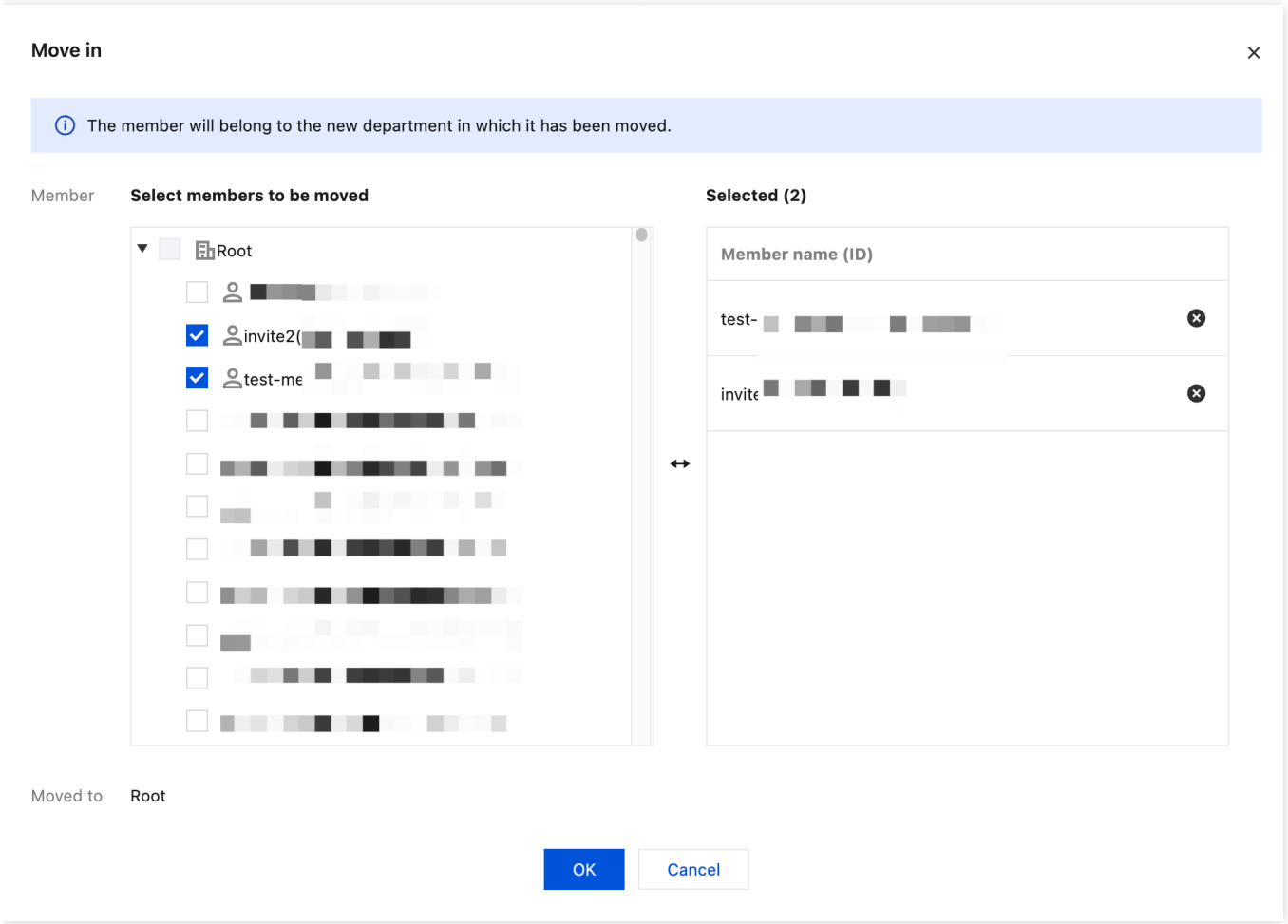
1. Log in to the Cloud Organization console. In the left sidebar, select Department Management.

2. In the window on the right of Department Management, perform the following operations as needed:

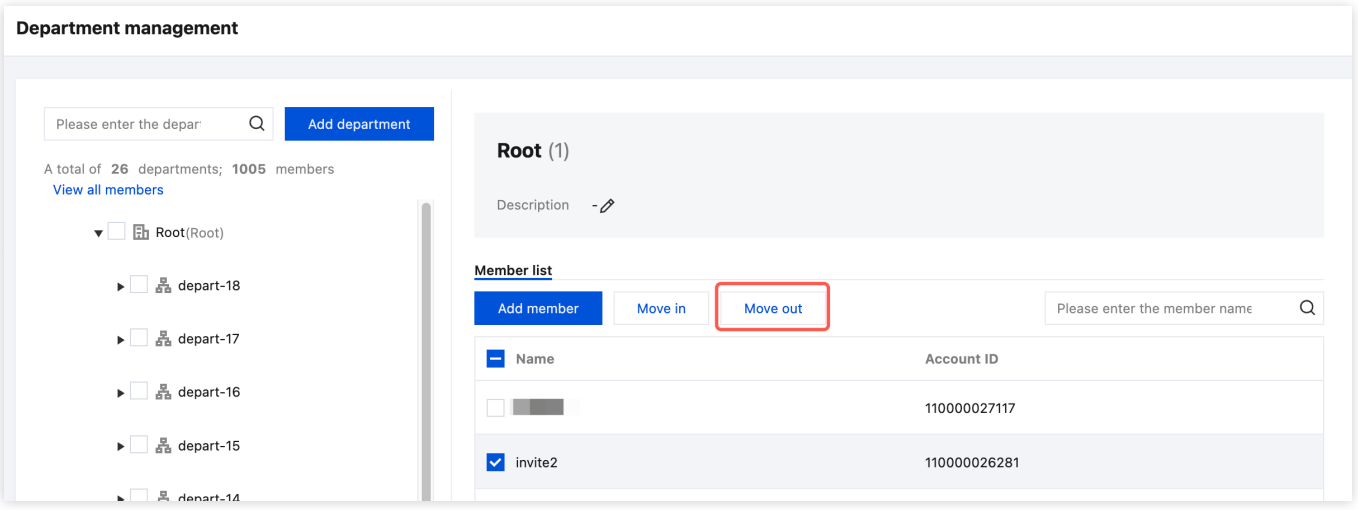
3. Click Move in on the Member list tab page on the right.



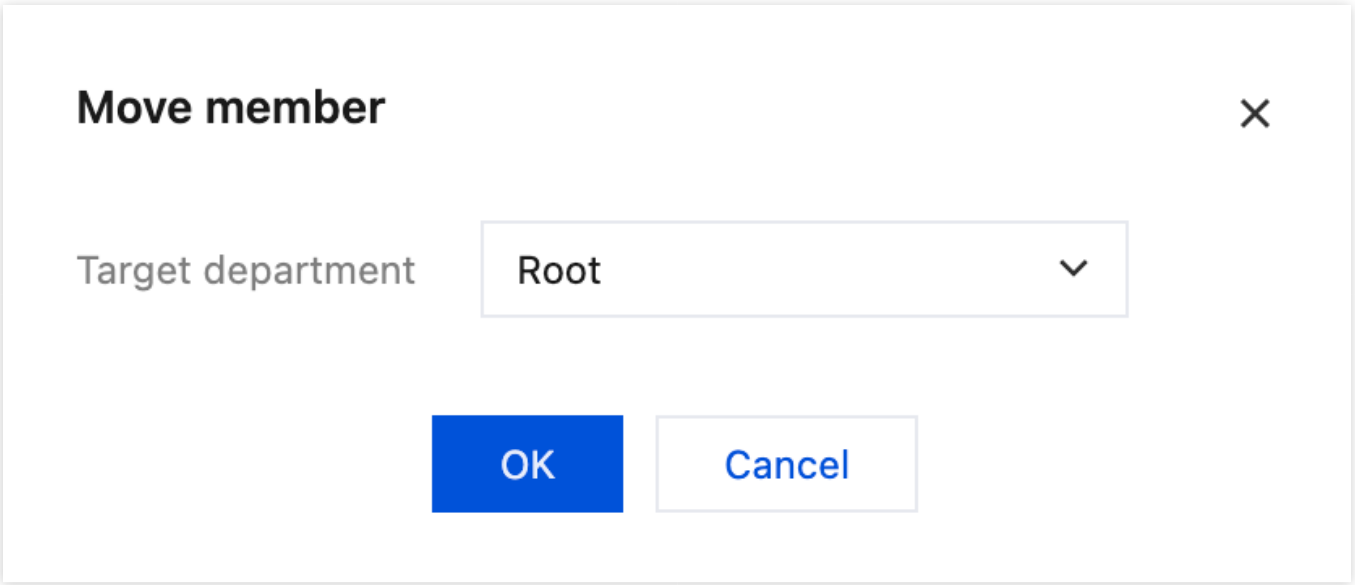
1. In the pop-up Move in Members window, select the members to be moved in, and click Confirm, as shown in the following figure:



1. Select the members to be removed on the Member list tab page on the right, and then click Move out.



2. In the pop-up Move member window, select the target department and click OK, as shown in the figure below:


Move member
Target department
Root
OK
Cancel

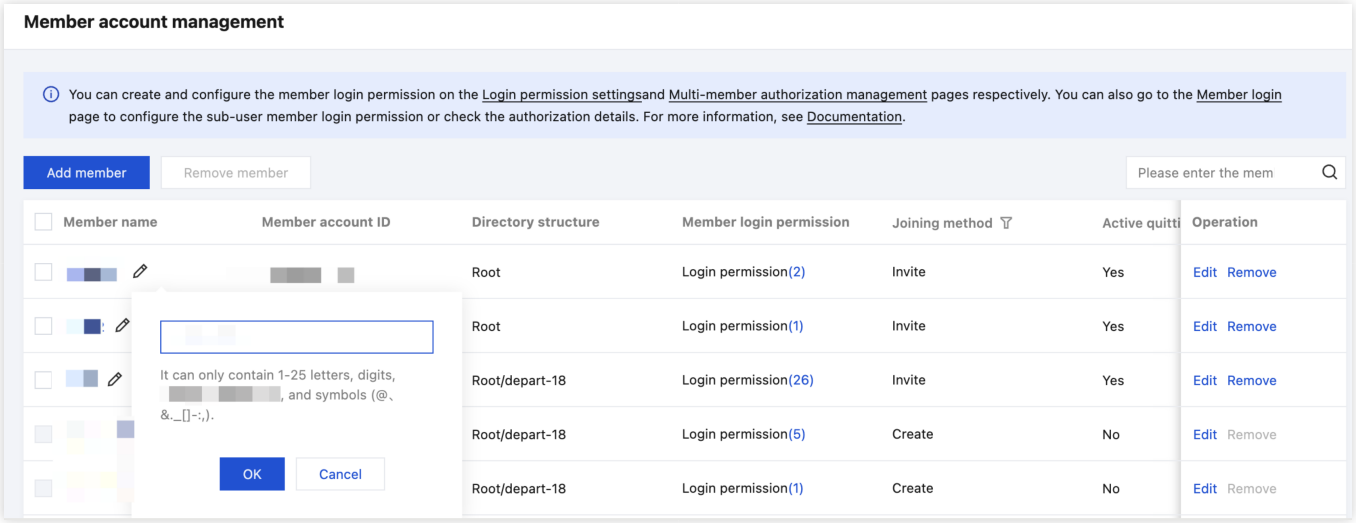
Member Account Management
Viewing or Editing Basic Member Information

This document introduces how to view or edit basic member information in the Cloud Organization console.

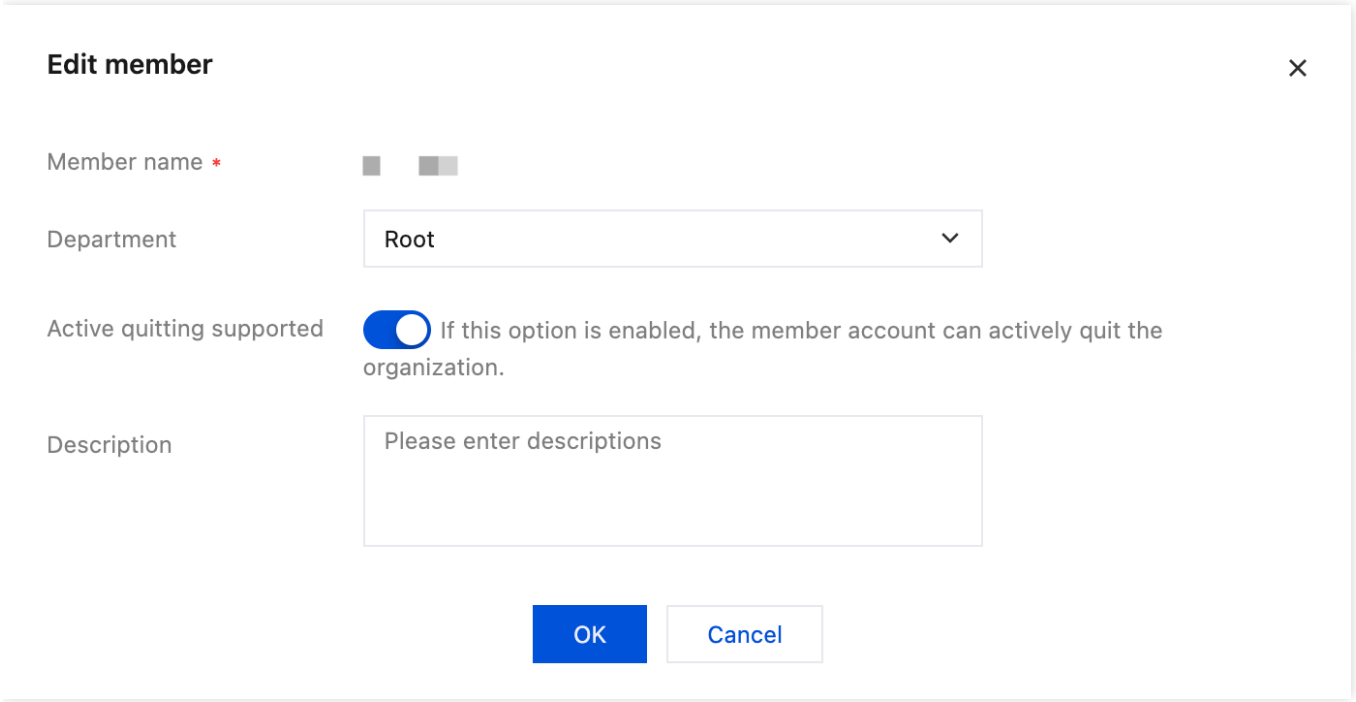
Operation Steps

1. Log in to the Cloud Organization console. In the left sidebar, select Member Account Management to view member information of the current group organization.
2. Member information includes the member name, member account ID, directory structure (department), member login permission, joining method, whether voluntary withdrawal is supported, and joining time. Among them, the member name, directory structure (department), member login permission, and whether voluntary withdrawal is supported can be modified.

3. On the Member account management page, click in the row of the member whose name needs to be modified.
4. Enter a new member name in the pop-up edit box and click OK to save the modification, as shown in the following figure:



5. To modify the directory structure (department), whether voluntary withdrawal is supported, or member description, click Edit in the Operation column on the right of the member row, and then modify the information in the pop-up Edit member window, as shown in the following figure:



6. To modify the login permissions for members, see Configuring Login Permissions for Members.

Removing Organization Members

This document introduces how to remove organization members from the Cloud Organization console.

Operation Steps

1. Log in to the Cloud Organization console. In the left sidebar, select Member Account Management.
2. You can remove a single member or remove members in batches:
    - Remove a single member: Click Remove in the Operation column in the row where the member to be removed is located, and then click OK in the pop-up dialog box.
    - Remove members in batches: Select the checkboxes on the left side of the member names, and then click Remove member above the member list.

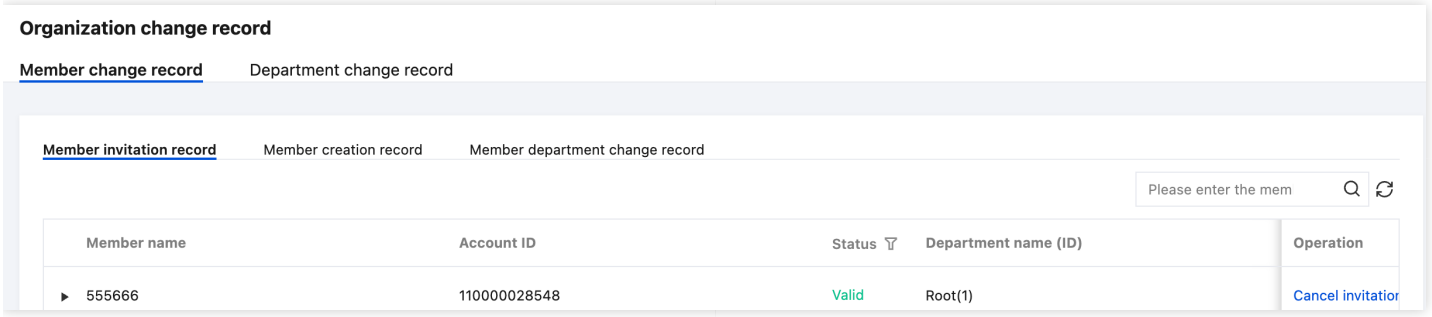
      > Note:
      >
      > - Removing a member only means removing the member from the organization. The member account can still log in to and use the cloud platform.
      > - After an organization member is removed, you cannot view or edit that member in the member list.

Adding an Organization Member

The group organization creator can add a member to the organization.

Operation Steps

1. Log in to the Cloud Organization console. In the left sidebar, select Member Account Management.
2. On the Member account management page, click Add member.
3. Fill in the account ID, member name, and department, and specify whether voluntary withdrawal is supported as needed in sequence.
4. After all information is specified, click OK. The information of the invited member needs to be verified. The invited account should not have joined any group organization before.
5. After the invitation is successful, the invitation message will be valid for 15 days. You can select Organization Change Record in the left sidebar. Then, choose Member change record > Member invitation record to view the invitation information, as shown in the following figure:

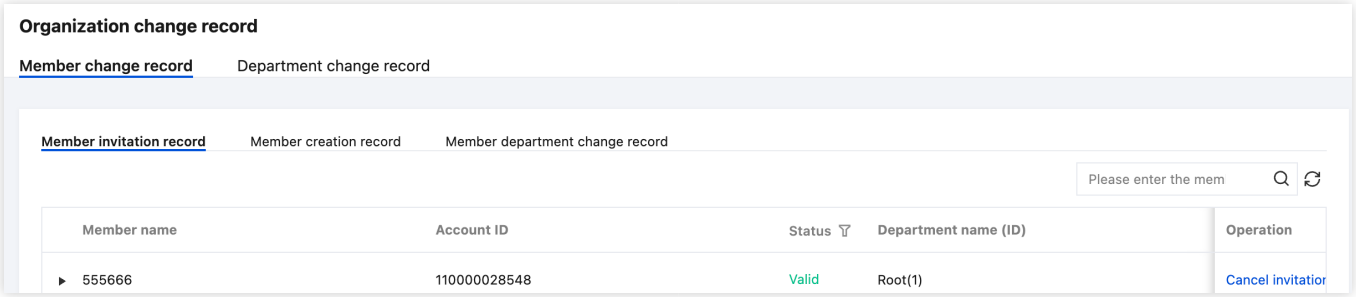


Canceling a Member Invitation

The group organization creator can cancel an invitation before it is accepted by the invitee.

Operation Steps

1. Log in to the Cloud Organization console. In the left sidebar, select Organization Change Records.
2. On the Organization Change Record page, choose Member change record > Member invitation record, and click Cancel invitation on the right side of the invitee row, as shown in the following figure:



3. In the pop-up dialog box, click OK to complete the cancellation.

Creating Member Login Permissions

Scenarios

In Cloud Organization, the group administrator can refine member permissions by creating a login permission. Sub-users granted login permissions can only log in to member accounts within the scope of their permissions. This document introduces how to create member login permissions in the Cloud Organization console.

Operation Steps

Creating Login Permissions

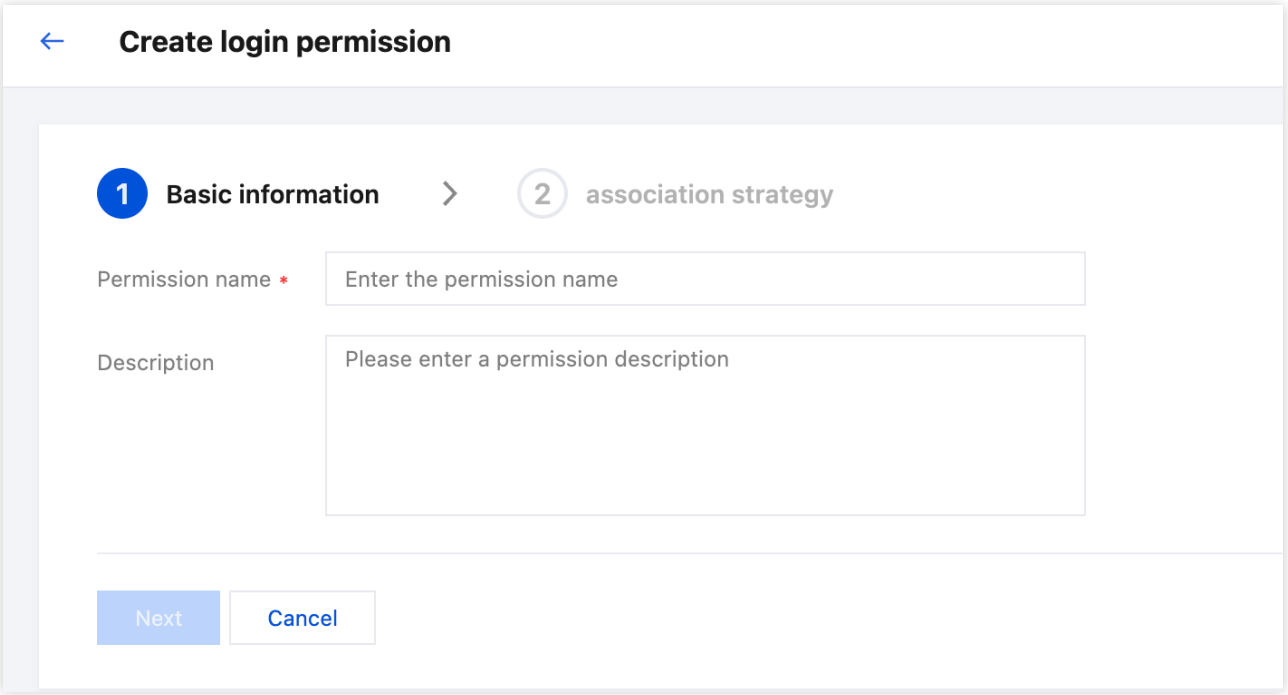
1. Log in to the Cloud Organization console. In the left sidebar, select Member Login Permission Settings.

2. Click Create login permission.

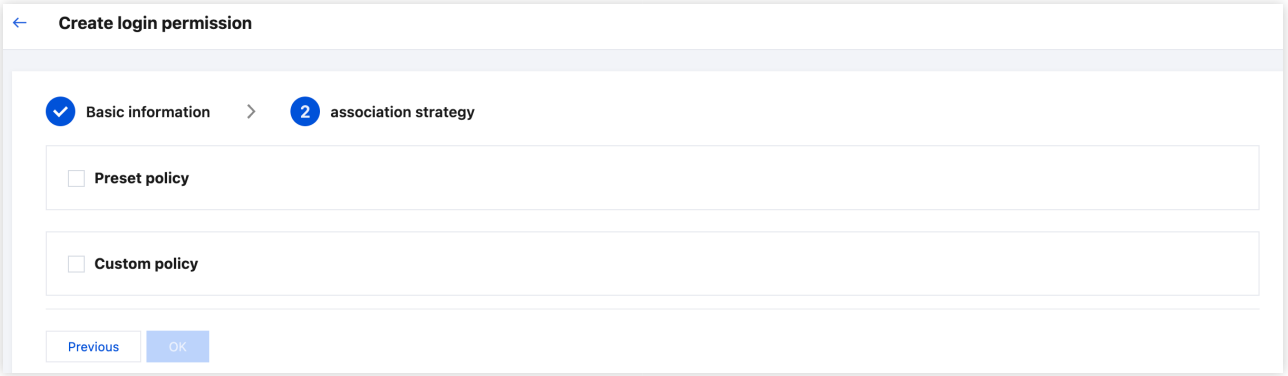
3. On the Create login permission page, set the permission name, description, and associated permission policy as needed.

   > Note
   >
   > Go to the Policy page to understand the specific meaning of the policy.

   i. Fill in the basic information of a login permission, including the permission name and description. The permission name is required, while the description is optional. After entering the basic information, click Next.



ii. Select a policy associated with the login permission. You can select a preset policy or a custom policy as needed (or both).



4. Click OK to successfully create the login permission.

> Note
>
> - Admin is the default permission, which allows member accounts to have the administrator permissions.

Configuring Login Permissions for Members

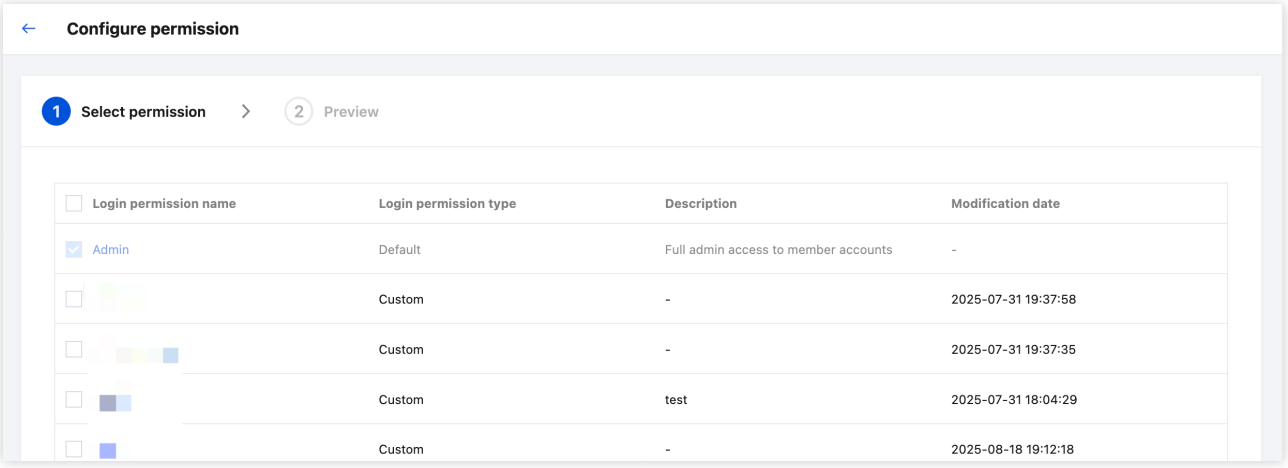
Scenarios

After creating login permissions, you can configure login permissions for members. This document introduces how to configure login permissions for members and delete member login permissions in the Cloud Organization console.

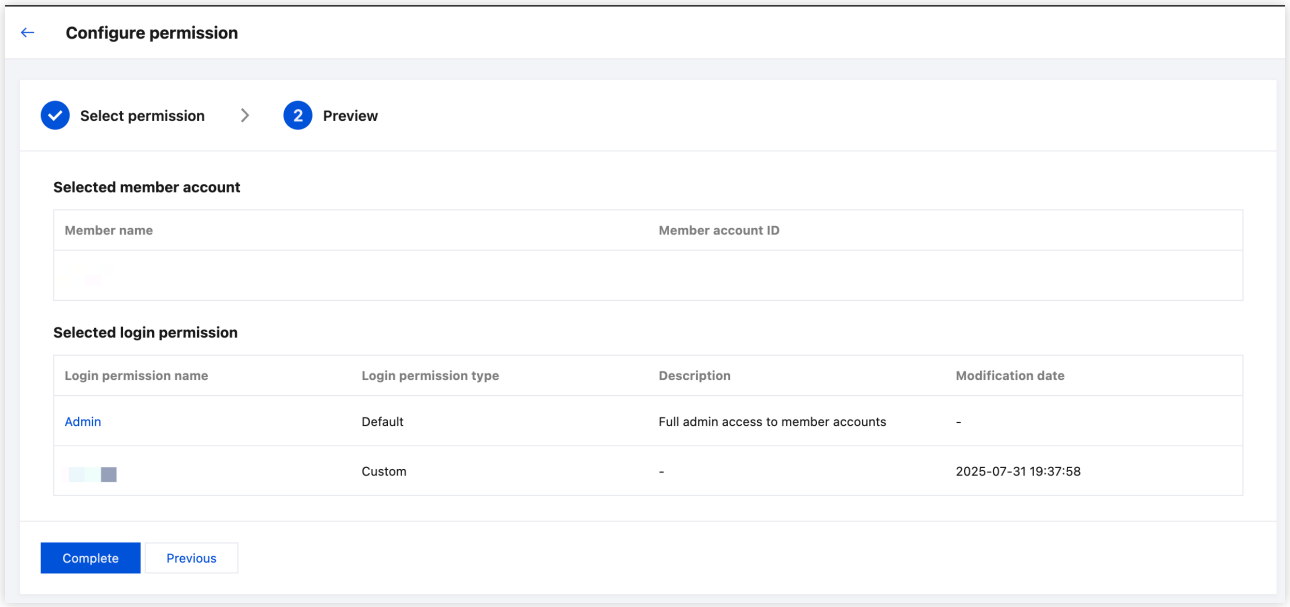
Operation Steps

Configuring Member Login Permissions

1. Log in to the Cloud Organization console. In the left sidebar, choose Unified Member Login > Multi-Member Authorization Management.
2. In the member list, select the members to configure permissions.
3. Click Configure permission.
    i. Select permissions.
    Select the permissions to be configured from the permission list, as shown in the figure below:



    ii. Preview and confirm the permissions.
    On the Preview page, confirm the member account and permission information, as shown in the figure below:

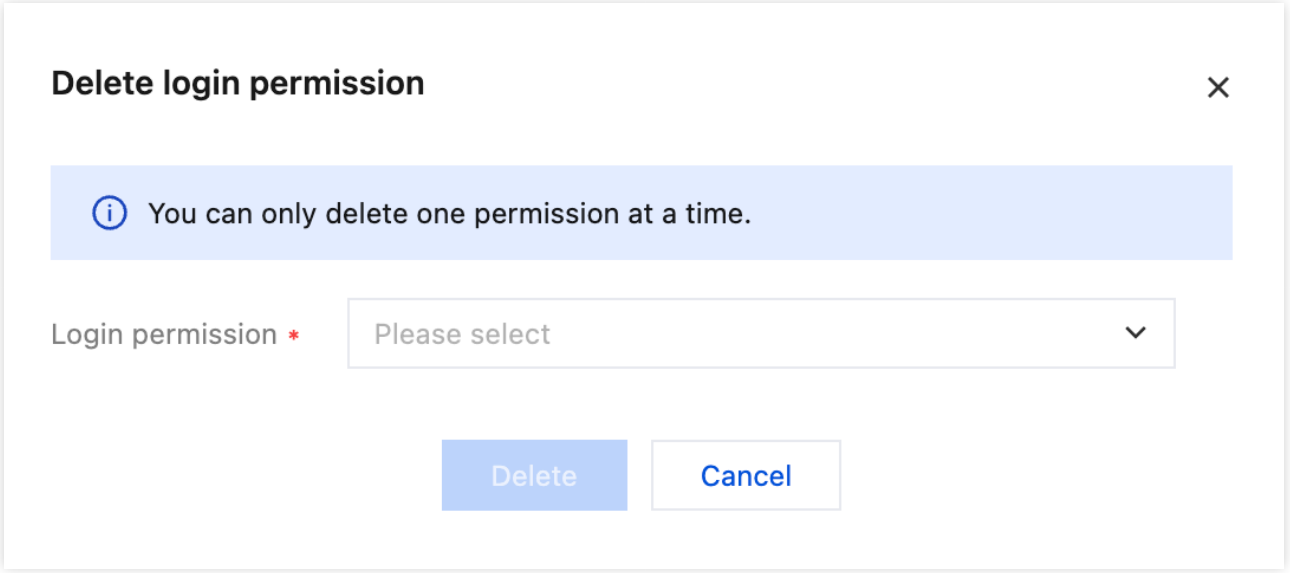


4. Click Complete to successfully configure login permissions for members.

Deleting Login Permissions

Method 1:

1. Log in to the Cloud Organization console. In the left sidebar, choose Unified Member Login > Multi-Member Authorization Management.
2. Select a member and click Delete permission in the Operation column.
3. In the pop-up Delete login permission window, select the permission to be deleted.

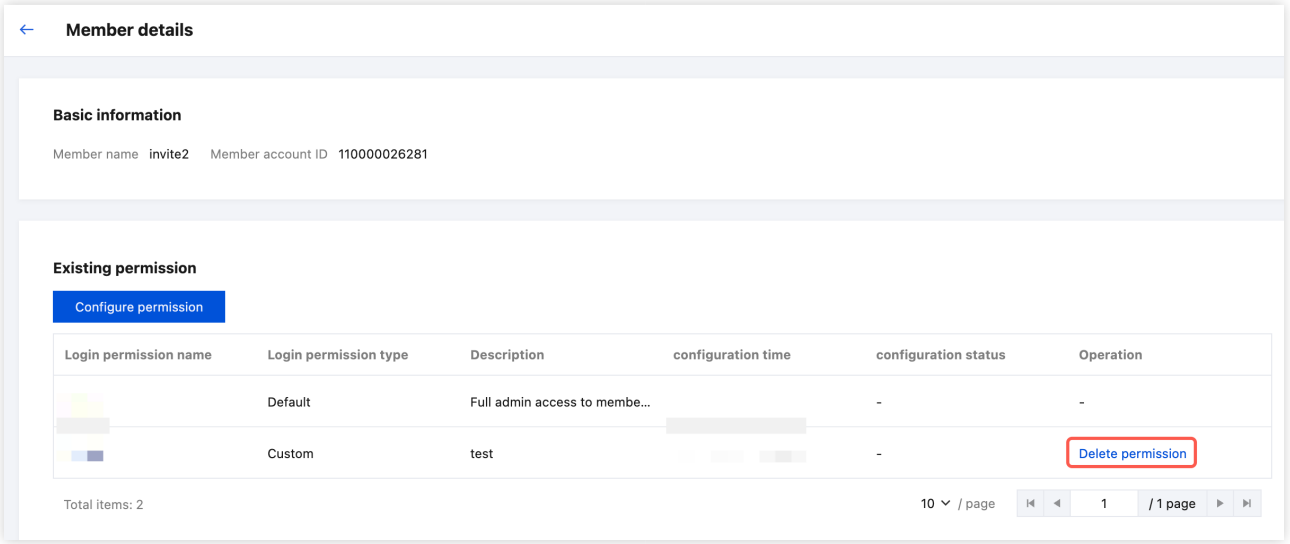


4. Click Delete to successfully delete the login permission.

Method 2:

1. Log in to the Cloud Organization console. In the left sidebar, choose Unified Member Login > Multi-Member Authorization Management.

2. Click a member name to go to the Member details page.
3. On the Member details page, select the permissions to be deleted and click Delete permission in the Operation column, as shown in the figure below:



4. In the pop-up window, click OK to successfully delete the login permission.

Authorizing Member Account Login

Scenarios

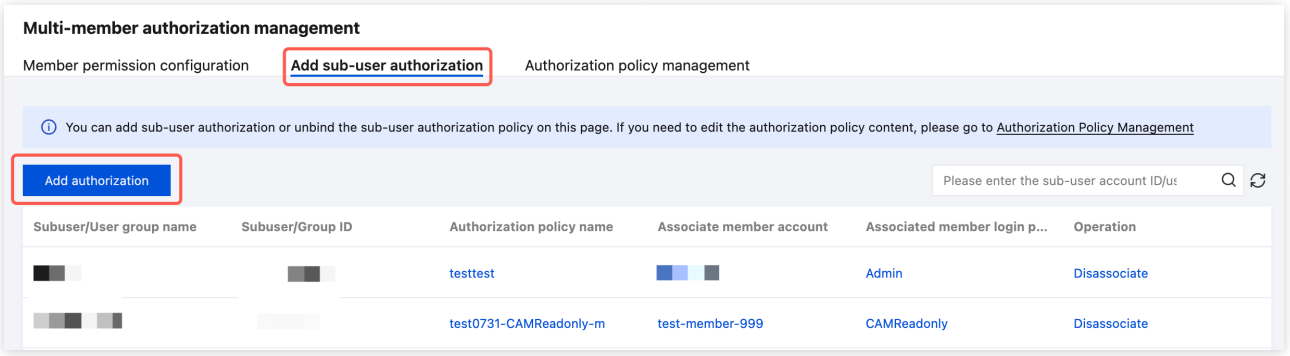
In Cloud Organization, the organization administrator can refine member permissions by creating login permissions. Sub-users who are granted login permissions can log in to member accounts only within the scope of their permissions. This document describes how to create member login permissions through the Cloud Organization console.

Operation Steps

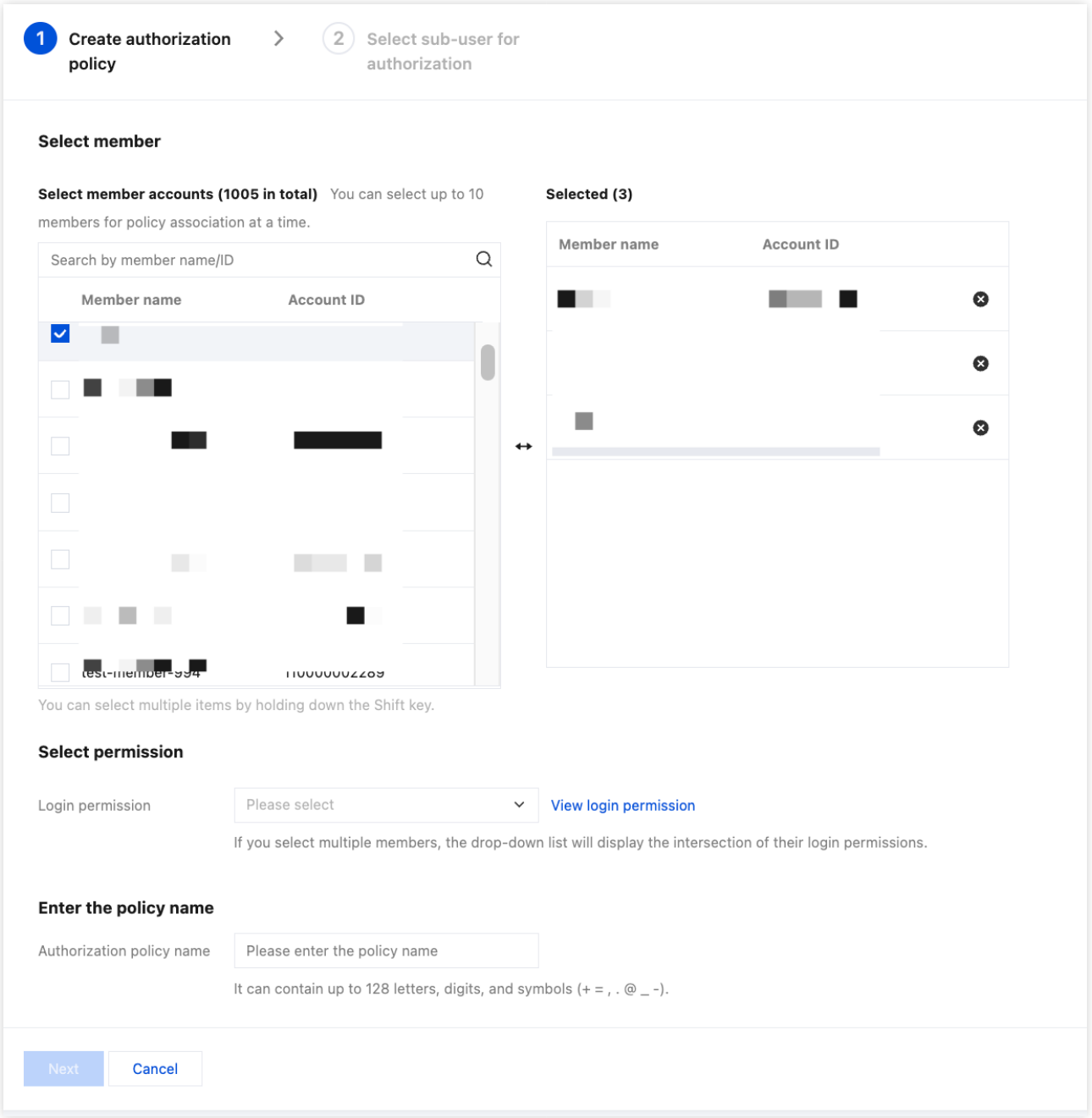
I. Adding Authorization

1. Log in to the Cloud Organization console. In the left sidebar, select Multi-member Authorization Management.

2. Click the Add Sub-user Authorization tab, and then click Add Authorization, as shown in the following figure:



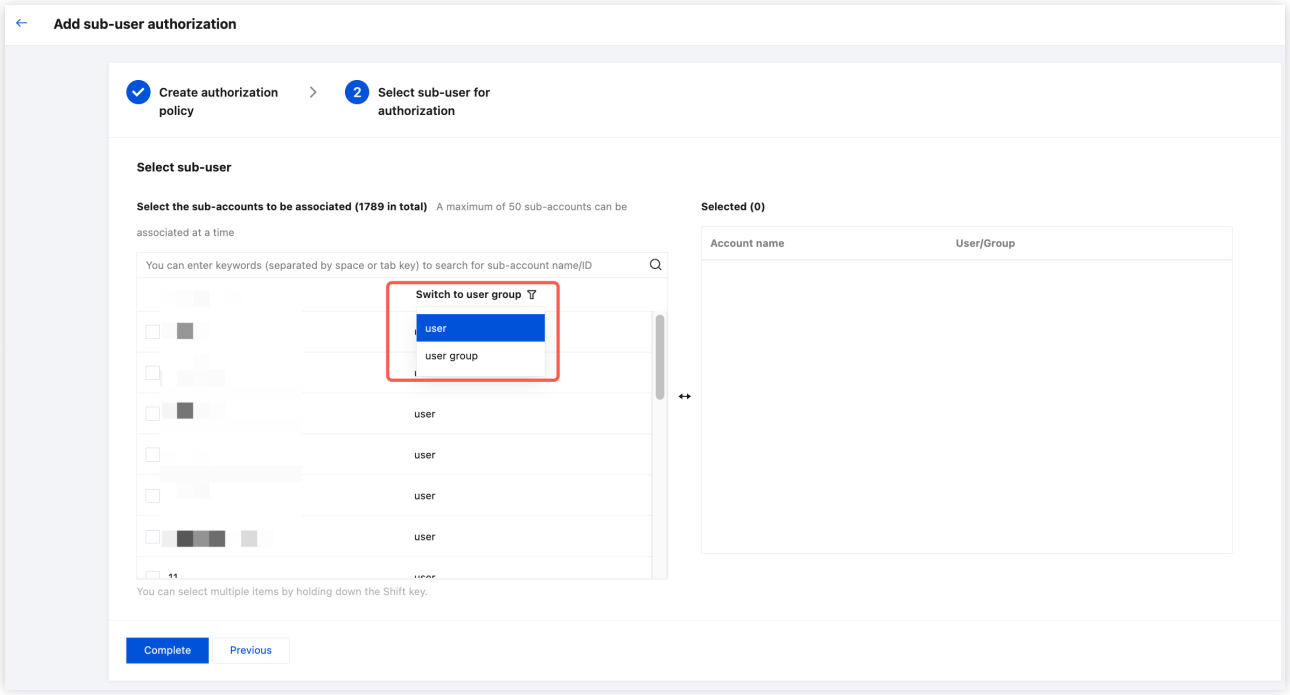
3. In the pop-up Add Authorization window, select members and the login permission and enter the authorization policy name in sequence, as shown in the following figure:



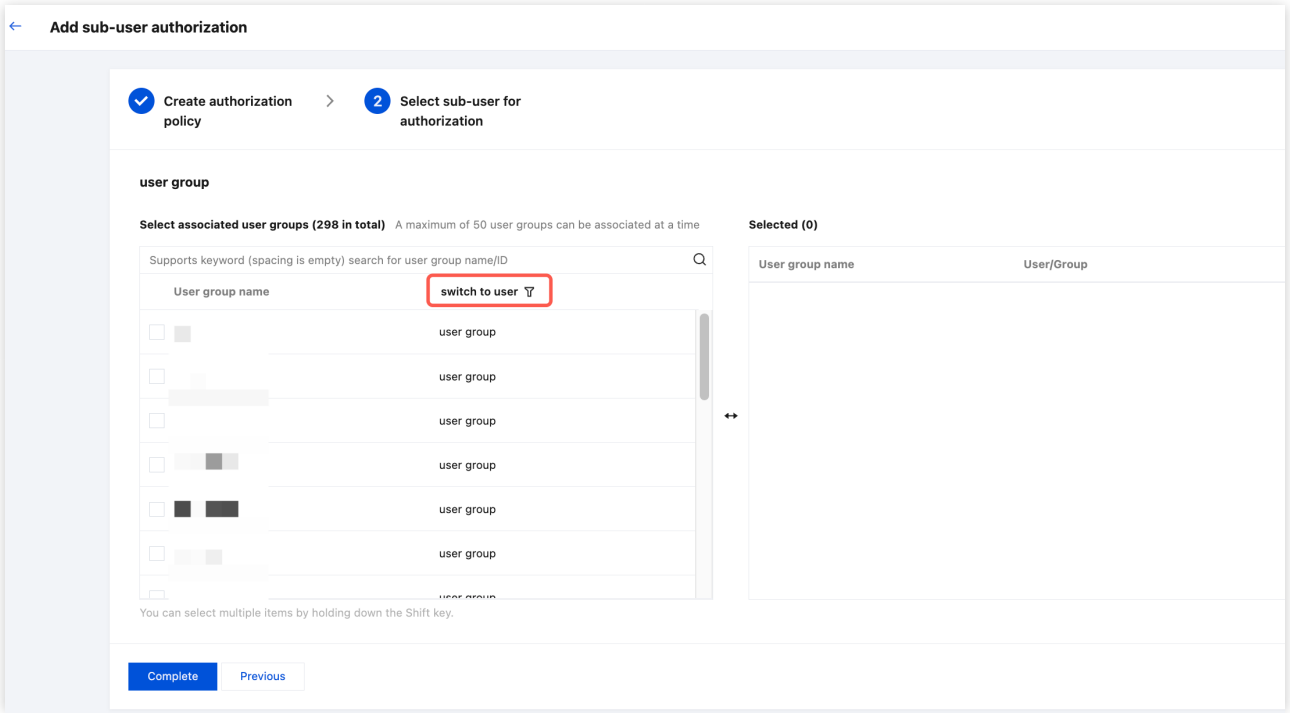
> Note:
>
> - The policy created in this step is a group management policy.
> - Group management policies cannot be modified or deleted in Cloud Access Management (CAM). If modifications are needed, go to Unified Member Login > Multi-member Authorization Management > Authorization Policy Management.
> - The authorization policy name should be unique.
> - When multiple members are selected, the Login Permission Drop-down List shows the intersection of the login permissions of the selected members. Only one login permission can be selected.

4. Click Next, select the sub-accounts to be associated as needed. Sub-users or user groups can be selected.
   - Sub-users are selected by default. If you need to select a user group, you can switch to the user group, as

shown in the following figure:



- After selecting a user group, you can also switch to sub-users, as shown in the following figure:



5. Click Complete to complete the authorization.

II. Logging in to a Member Account with a Sub-account

After the authorization is complete, you can log in to a member account with the corresponding sub-account and perform management operations.

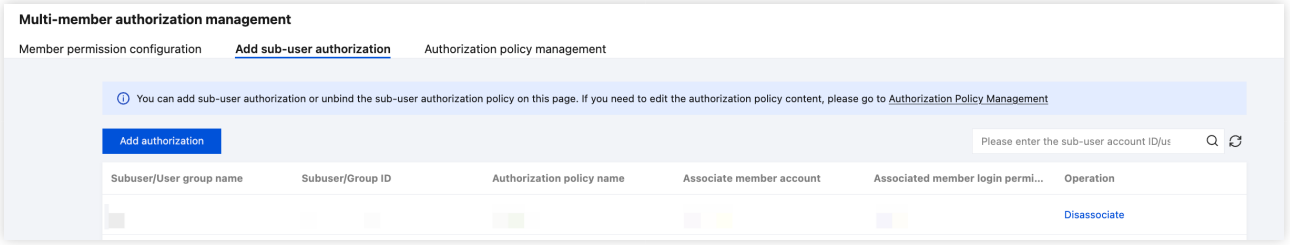
1. Log in to the Cloud Organization console with an authorized sub-account. In the left sidebar, select Member Login.

2. On the Member Login page, select the member account you want to log in, click Login Account in the Operation column, and select a login permission from the pop-up Login Member Account window, as shown in the following figure:

> Note:
>
> - You can only select one permission to log in each time.
> - You can only authorize a sub-account of the admin account to log in to a member account.

III. Revoking Authorization

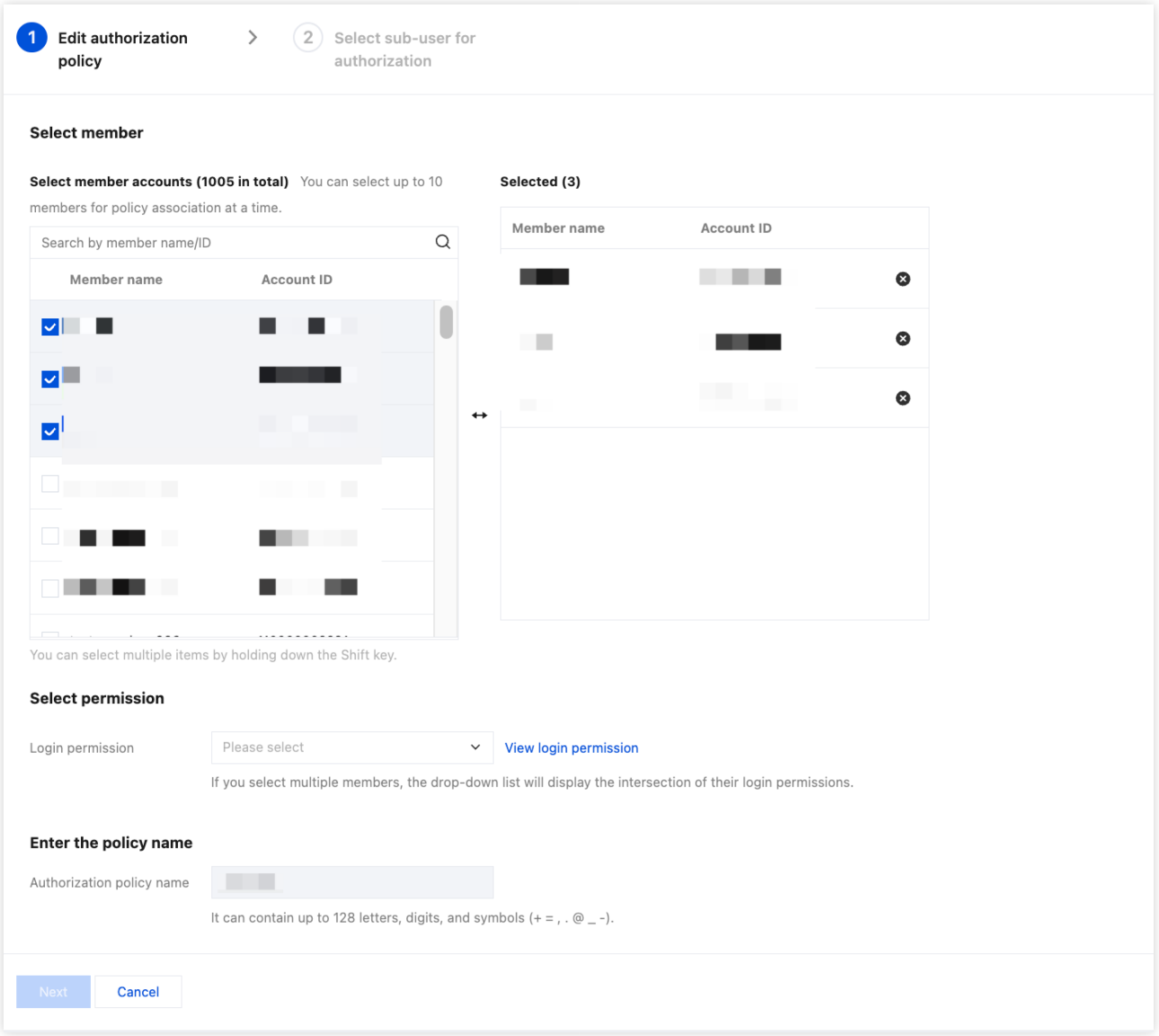
1. Log in to the Cloud Organization console. In the left sidebar, select Multi-member Authorization Management, and then click the Add Sub-user Authorization tab.
2. On the Add Sub-user Authorization page, click Unbind in the Operation column.



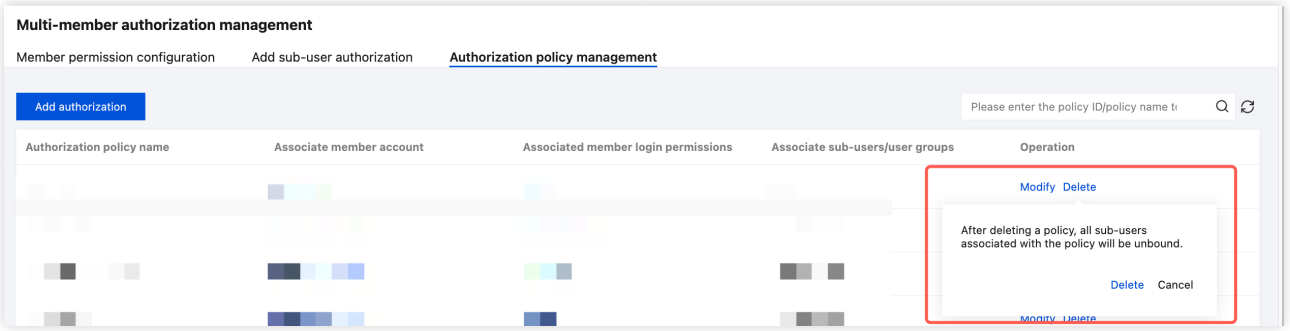
3. Click Confirm to revoke the authorization.

IV. Modifying or Deleting a Group Management Policy (Authorization Policy)

1. Log in to the Cloud Organization console. In the left sidebar, select Multi-member Authorization Management, and then click the Authorization Policy Management tab.
2. On the Authorization Policy Management tab, click Modify in the Operation column to modify the policy content on the corresponding page. The policy name cannot be modified.



3. On the Authorization Policy Management tab, click Delete in the Operation column, and then click Confirm Deletion in the pop-up window to delete the corresponding authorization policy.

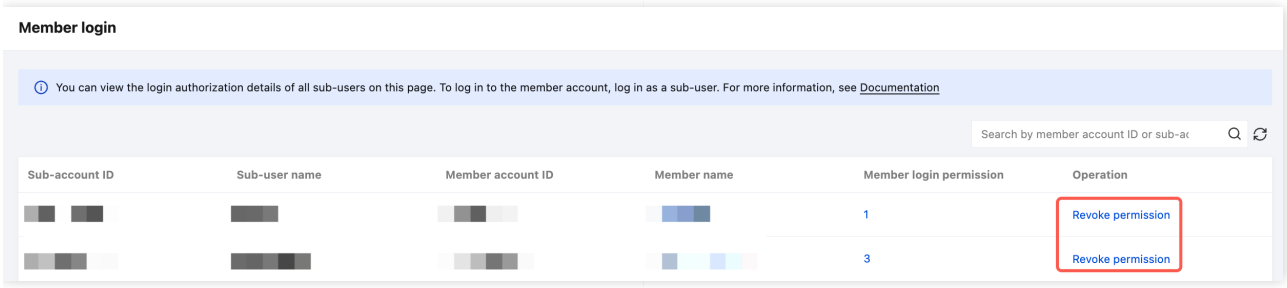


V. Managing Sub-account Permissions to Log in to Member Accounts

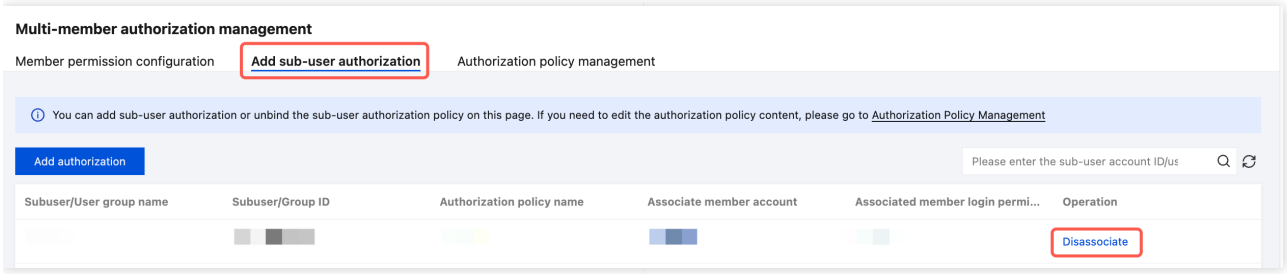
The root account user of the group admin account can view the list of all sub-accounts that can log in to member accounts, and have the authority to revoke the permissions of sub-accounts.

1.Log in to the Cloud Organization console. In the left sidebar, select Member Login.

2.On the Member Login List page, select a member and click Revoke Permission in the Operation column.



3.Alternatively, select Multi-member Authorization Management in the left sidebar. On the Add Sub-user Authorization page, click Unbind in the Operation column.



4.Click OK to successfully revoke the permission.

Member Financial Management
Organization Finance Overview

Organization Finance Overview allows the admin account to view and manage an enterprise's consumption of admin accounts by dimensions such as member and product. The enterprise admin account can centrally view and manage the consumption of all accounts within an enterprise, enhancing the financial management efficiency of the enterprise.

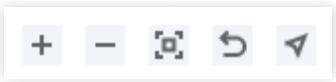
> Note:
>
> - Group bill overview is provided one day after the transaction date, known as T+1. It is recommended to view the group bill overview for the current month after 15:00.
> - A monthly group bill is issued on the 2nd day of the next month. It is recommended to view the complete bill issued for the previous month after 19:00. To view the detailed bill, go to Billing Management in the tenant-side navigation menu.
> - Organization Finance Overview only displays financial data on self-payment of the admin account/member accounts in the past six months. Data before organization creation is not displayed. If a member joins the group after the 1st day of the current month, the financial data of that member for the current month is not visible (except for the admin account).

Operation Steps

Viewing the Group Finance Architecture Diagram

1. Log in to the Cloud Organization console. In the left sidebar, choose Financial Management > Organization Finance Overview.

2. On the Organization Finance Overview page, you can view the Group Financial Structure.

3. Click  to zoom in, zoom out, fit-to-canvas, undo operations, or open the navigation bar.

4. Click Hide Financial Structure to hide the architecture diagram. If you need to view it again, click  to display the Group Financial Structure.

Viewing Fee Trends and Bill Details

1. Log in to the Cloud Organization console. In the left sidebar, choose Financial Management > Organization Finance Overview.

2. Select a duration at the top of the Organization Finance Overview page, and select members and products in the Fee Trend module. Then, the corresponding fee trends and bill details are displayed.

   > Note:
   >
   > - On the Organization Finance Overview page, the financial overview details of all members and products in the past six months are displayed by default.
   > - A time interval of up to 6 months can be selected for fee information display. If this interval is exceeded, the information will not be displayed.

3. In the Fee Trend module, you can view the fee trend charts for the selected members and products in the selected time period, as well as the specific consumption amount in each month and the average total monthly fee.

4. In the Bill Detail module, you can view the fee details for the selected members and products in the selected time period. In the upper-right corner, you can choose to display information by member or by product as needed.

   (1) If you choose to display information by member:

   - A pie chart of the top 5 member accounts by total consumption amount is displayed at the top, and the member account names and corresponding amounts and proportions are displayed on the right.
   - A financial list of the selected members is displayed at the bottom, including the member account ID, member account name, time, total fee, consumption proportion, and details. Click Consumption Details to show the product consumption distribution chart of a member in the specified time period.

   (2) If you choose to display information by product:

   - A pie chart of the top 5 products by total consumption amount is displayed at the top, and the product names and corresponding amounts and proportions are displayed on the right.
   - A financial list of the selected products is displayed at the bottom, including the product name, time, total fee, consumption proportion, and details. Click Details to show the member consumption distribution chart of a product in the specified time period.

Identity Center Management
Introduction to Identity Center
Introduction to Identity Center

Identity Center provides unified identity and permission management for multiple accounts based on the cloud organization structure. Using the Identity Center feature of Cloud Organization, you can centrally manage cloud platform users of your enterprise, configure Single Sign-On (SSO) between the enterprise identity management system and the cloud platform, and centrally configure user access permissions on multiple accounts.

Features

- Unified management of cloud platform users
  Identity Center offers you a user management module where you can maintain all users who need to access the cloud platform. 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.
- Unified configuration of 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.
- Unified configuration of user access permissions on multiple accounts
  By leveraging the structure of your cloud organization, you can centrally configure user or user group permissions to access 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 cloud platform console and easily switch between multiple accounts.

Relationship Between Identity Center and CAM

- Cloud Access Management (CAM) supports identity and permission management of individual cloud platform accounts. It offers user management (including users, user groups, and roles), SSO, and permission configuration, which are only effective on individual cloud platform accounts. When your

enterprise has multiple cloud platform accounts, you need to use CAM to manage users of each account separately and to configure SSO and permissions separately, which poses significant management challenges.

- Identity Center provides unified identity and permission management for multiple accounts of an organization. With Identity Center, you can perform unified configuration, achieving user management and SSO for multiple cloud platform accounts. To achieve this, Identity Center offers identity management independent of CAM, but its permission configuration feature reuses the permission policies in CAM. In addition, the access of Identity Center users to accounts is essentially another SSO performed by Identity Center users assuming the CAM role of each account.
- When you start using Identity Center for unified identity and permission management of your cloud organization, you no longer need to use CAM to manage individual accounts. However, in certain cases, you can still use CAM on individual accounts. For example, you have existing CAM users and CAM roles, or you need to use access keys for programmatic access to cloud platform resources. Using Identity Center does not restrict the original features of CAM. Both services can be used simultaneously.

Basic Concepts

This document introduces the basic concept of Identity Center.

Concept	Description
Space	To enable Identity Center, you need to create a space. All resources of Identity Center are maintained in this space. For a cloud organization, only one space can be created. The space name will be used in the user login URL.
User	User is an identity type in Identity Center. It means that if you enable the Identity Center service of Cloud Organization, before the CAM synchronization operation is performed, the user you created in Identity Center has no feature, identity, or permission such as login or access. You can centrally create and manage users accessing the cloud platform. Users can be granted permissions to access the cloud platform account.
User group	User group is an identity type in Identity Center. You can add users to user groups and grant users permissions by user group for unified permission management.
SCIM synchronization	Identity Center supports user and user group synchronization based on the SCIM protocol. With SCIM synchronization, you only need to manage identities in your enterprise identity management system, eliminating the need for manual management of users and user groups in Identity Center. This enhances management efficiency and security.
Account	Accounts include an admin account and member accounts. - Admin account: The admin account is the super administrator of an enterprise organization. Only the admin account can manage Identity Center. - Member account: A member account cannot manage Identity Center and cannot be viewed.
Multi-account authorization	According to the structure of your cloud organization, you can set users or user groups allowed to be accessed by each account, as well as their access permissions. You can authorize the enterprise admin account or any member account. For more information, see Multi-account Authorization Overview.
Login portal	The login portal is an independent portal for Identity Center users to log in to the cloud platform and use the cloud platform resources. After logging in, Identity Center users can view the accounts with the access permission and only access the cloud platform console within the scope allowed by the granted permissions. You can view the URL of the login portal on the Overview page of Identity Center. For more information, see Identity Center User Login.
Identity Center administrator	Identity Center administrators refer to the admin account for which Identity Center is enabled and CAM users with the QcloudOrganizationFullAccess permission under the admin account.

Concept	Description
Single sign-on (SSO)	Identity Center supports SSO based on SAML 2.0. The cloud platform is a service provider (SP), and the identity management system of enterprises is an identity provider (IdP). Through SSO, enterprise employees can directly log in to Identity Center with their user identities in the IdP.

Identity Center Use Cases
Logging In with a Cloud Platform Sub-account

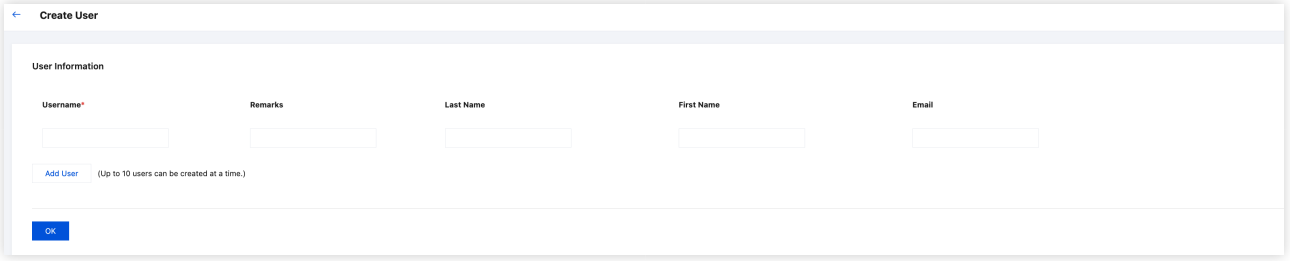
This document provides an example of creating a CAM sub-account (user1) with the same name as an Identity Center user (user1) in a member account (member_1) by configuring CAM user synchronization.
The sub-account created through CAM user synchronization is granted no permissions. You should grant permissions to the user in the CAM console for the member account.
If you need to preset permissions through Identity Center, select Configure CAM User Synchronization.

Operation Steps

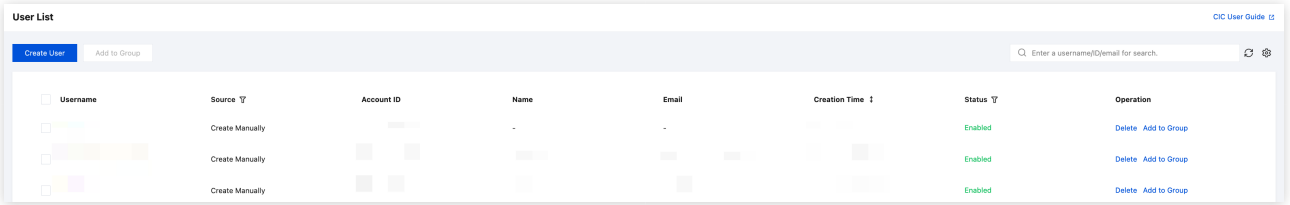
Step 1: Inputting Enterprise Employee Information

Input enterprise employee information into the User Management module of Identity Center. Currently, only manual creation is supported, which indicates that you need to create Identity Center users manually.

1. Go to Cloud Organization > Identity Center.
2. In the left sidebar, choose User Management > User.
3. On the Create User panel, set basic user information.



   - Username: required. The username should be unique within the space. The username can contain up to 64 characters, including English letters, digits, plus signs (+), equal signs (=), commas (,), periods (.), at signs (@), hyphens (-), and underscores (_). This parameter is set to user1 here.
   - Remarks, Last Name, First Name, and Email: optional. You can specify them as needed.
4. Click Confirm to complete the creation.



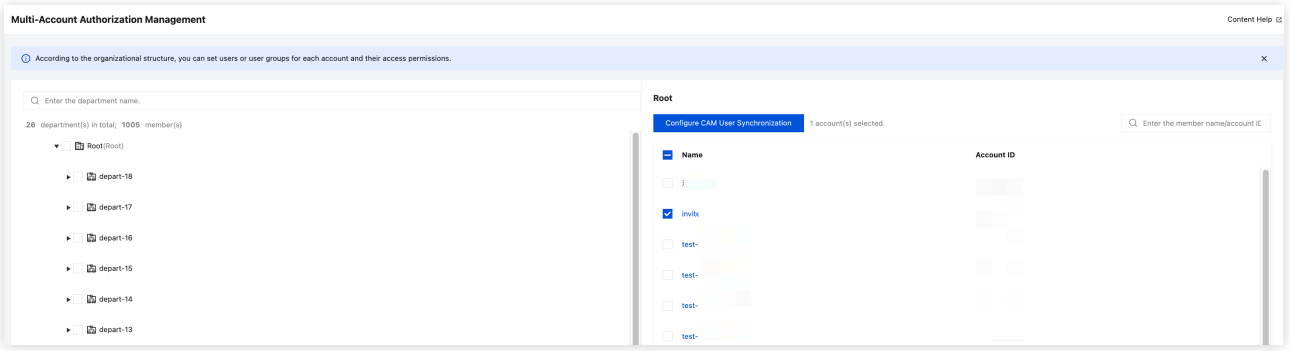
Step 2: Configuring CAM User Synchronization

1. In the left sidebar, click CAM Sync > Multi-account Authorization Management.

2. On the Multi-account Authorization Management page, select a target account.

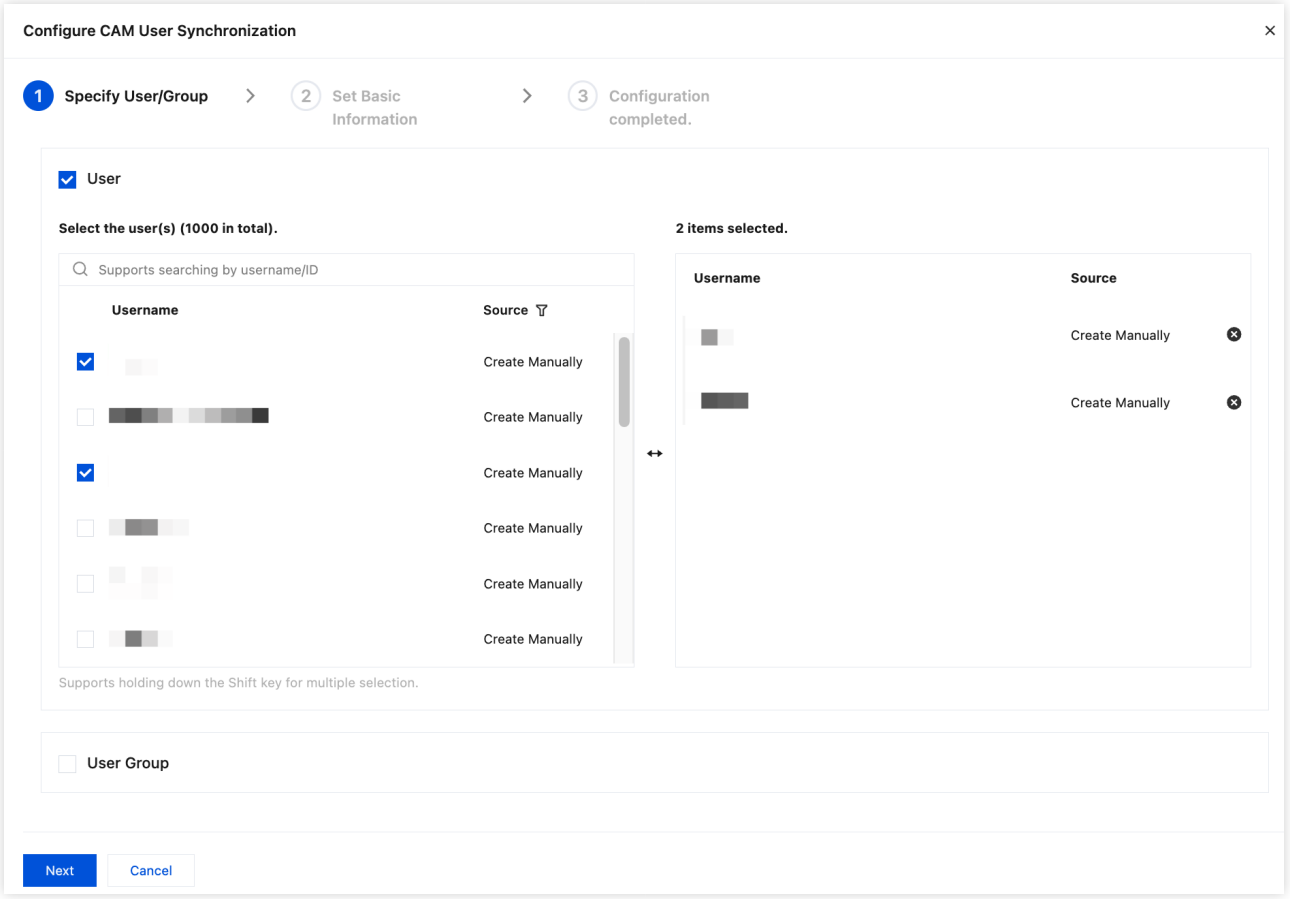
> Note:
>
> In this example, a member account (member_1) is selected.

3. Click Configure CAM User Synchronization.

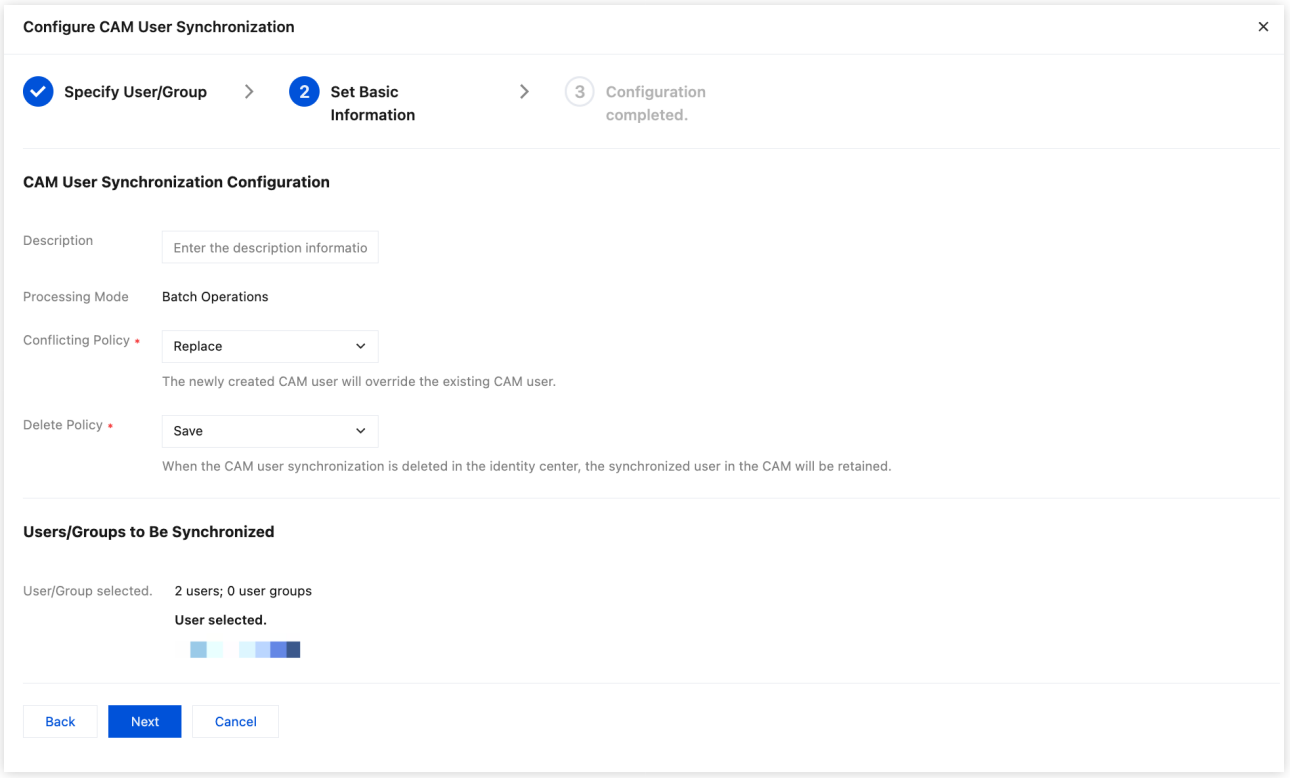


4. On the Configure CAM User Synchronization panel, select a target user or user group, and click Next.

> Note:
>
> In this example, an Identity Center user (user1) is selected.



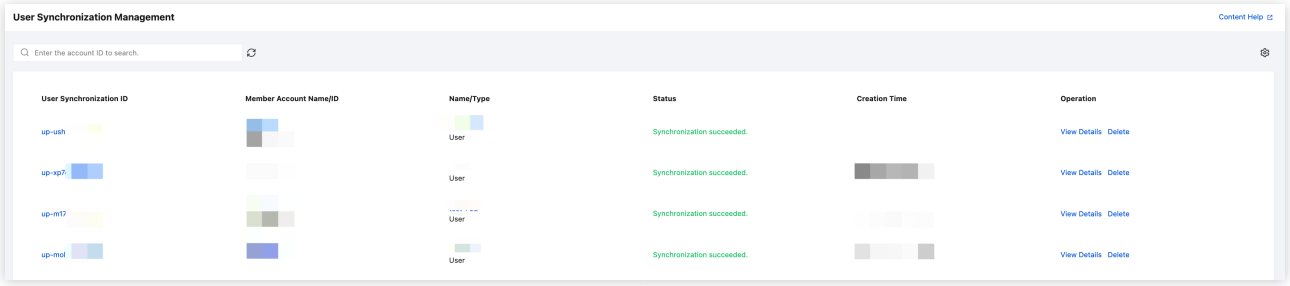
5. Set basic information. For details, see Configure CAM User Synchronization. After filling in the basic information, click Next.



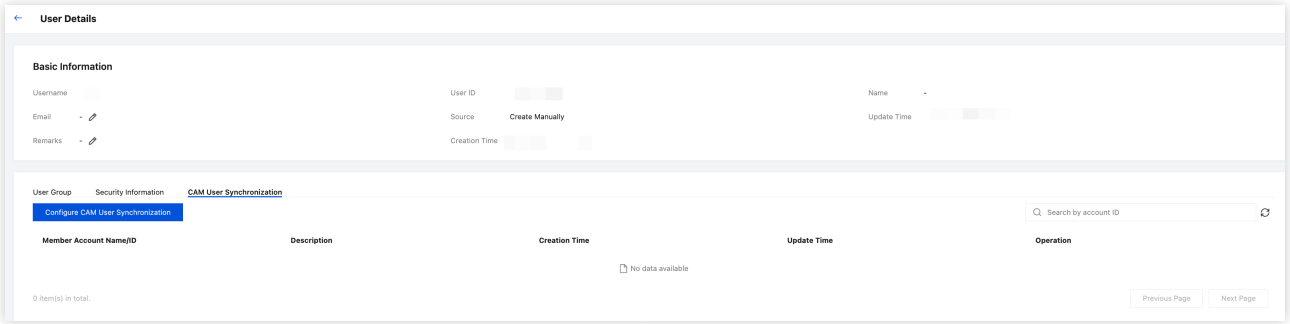
6. Click Submit. After receiving a prompt for successful configuration, click Done.

7. After successful configuration:

   - You can choose CAM Sync > User Synchronization Management to view the user synchronization list.



   - Alternatively, you can click User Management > Users, go to the user details page of user1, and then select the CAM User Synchronization tab to view the user synchronization list.



Effect in CAM

1. After successful configuration, the system will automatically create a CAM sub-user (user1) with the same name as the Identity Center user (user1) in the member account (member_1) through synchronization.

   > Note:
   >
   > The user type in CAM is Identity Center synchronized user.

2. Click the target username to view the associated policies.

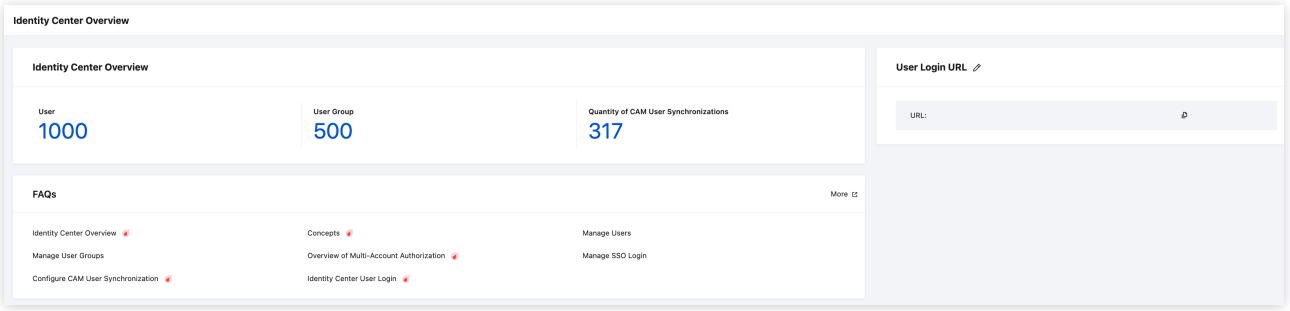
   > Note:
   >
   > The sub-user created through synchronization has no permissions. You need to configure permission policies for the user (user1) in CAM.

Step 3: Logging In with a Sub-account

Obtain the user login URL

1. In the left sidebar, click Identity Center Overview.

2. On the right side of the overview page, view or copy the user login URL.



Visit the user login URL in a browser

3. On the Identity Center Login page, click Login.

   > Note:
   >
   > Currently, only user-based SSO is supported. Account password login is not supported. You need to

> configure SSO by referring to Managing SSO first.

4. The system automatically redirects to the enterprise IdP Login page.

5. After verification is passed, go to the CAM User Login tab, and select a member account (member_1) for login.

Enabling a Service

Identity Center can be used after being enabled. After enabling it, you can use this service for free.

Prerequisites

The Cloud Organization service has been enabled, and a multi-account organizational structure for the enterprise has been set up.
Only the admin account of the cloud organization or the authorized CAM users under the admin account can enable Identity Center. The details are as follows:

- Admin account (root account)
- CAM users (sub-accounts)
- You need to grant the preset policy OrganizationFullAccess to the CAM users under the admin account.

Operation Steps

1. Log in to the Cloud Organization console.
2. In the directory of the Cloud Organization console, click Identity Center Overview.
3. On the Identity Center Overview page, click Enable Now.
4. When enabling Identity Center, fill in a space name, which should be globally unique.
    - The space name will be used in the user login URL later, and cannot be modified.
    - During the process of creating a space, Identity Center automatically creates a service-related role (Organization_QCSLinkedRoleInCIC) for accessing your resources in other cloud services.
5. Click OK.

Managing Users

Scenarios

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

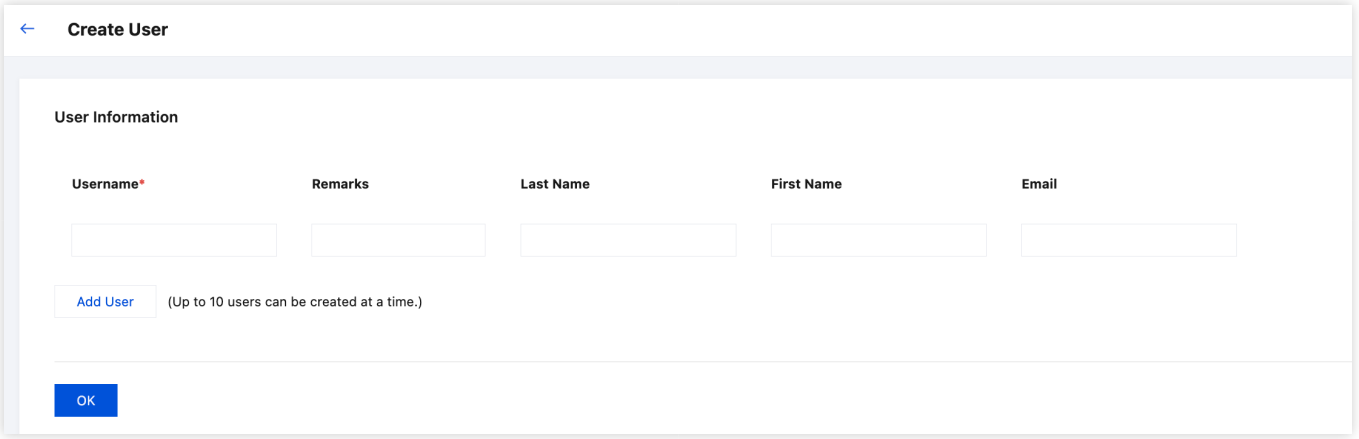
Prerequisites

You have logged in to Cloud Organization > Identity Center.

Operation Steps

Creating a User

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



   - Username: required. The username should be unique within the space. The username can contain up to 64 characters, including English letters, digits, plus signs (+), equal signs (=), commas (,), periods (.), at signs (@), hyphens (-), and underscores (_).
   - Remarks, Last Name, First Name, and Email: optional. You can specify them as needed.
4. Click OK.

Viewing User Information

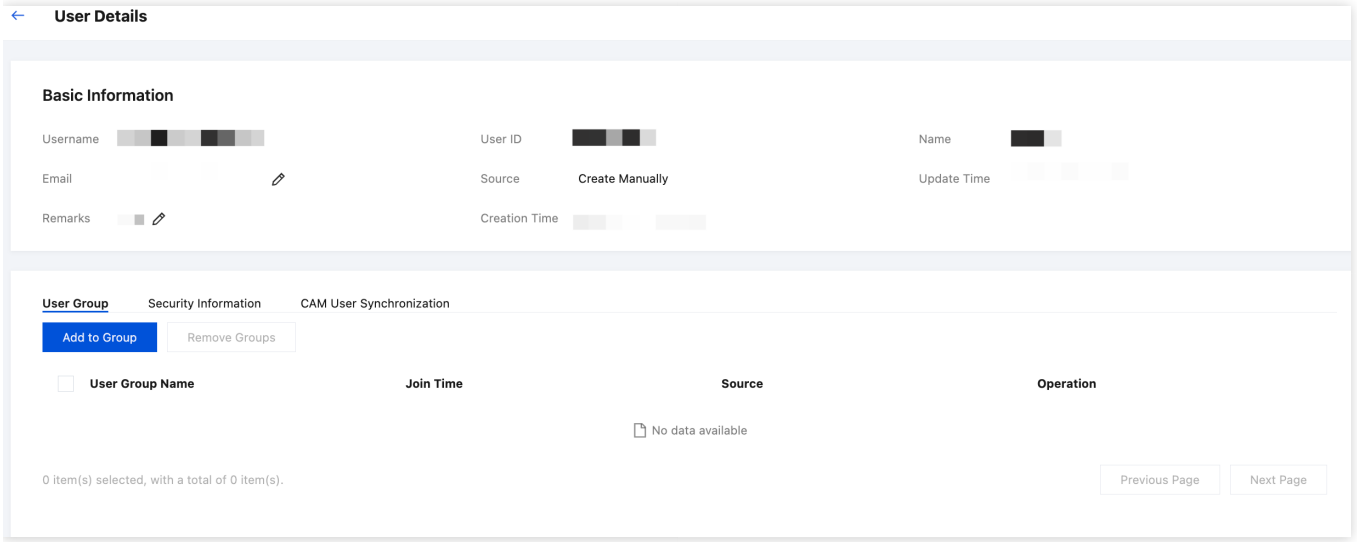
1. In the left sidebar, choose User Management > User.
2. On the User list page, click the target username to view the following information of the user:
   - View basic information of the user.

- Click the User Group tab to view the user groups the user has joined.
- Click the Security Information tab to view the enabling status of the user.
- Click the CAM User Synchronization tab to view the CAM user synchronization information configured for the user. For more information about CAM user synchronization, see Multi-account Authorization Overview.

Modifying Basic User Information

> Note:
>
> The username cannot be modified.

1. In the left sidebar, choose User Management > User.
2. On the User list page, click the target username.
3. In the Basic Info area at the top of the user details page, the modifiable fields are Remark and Mailbox.



Deleting a User

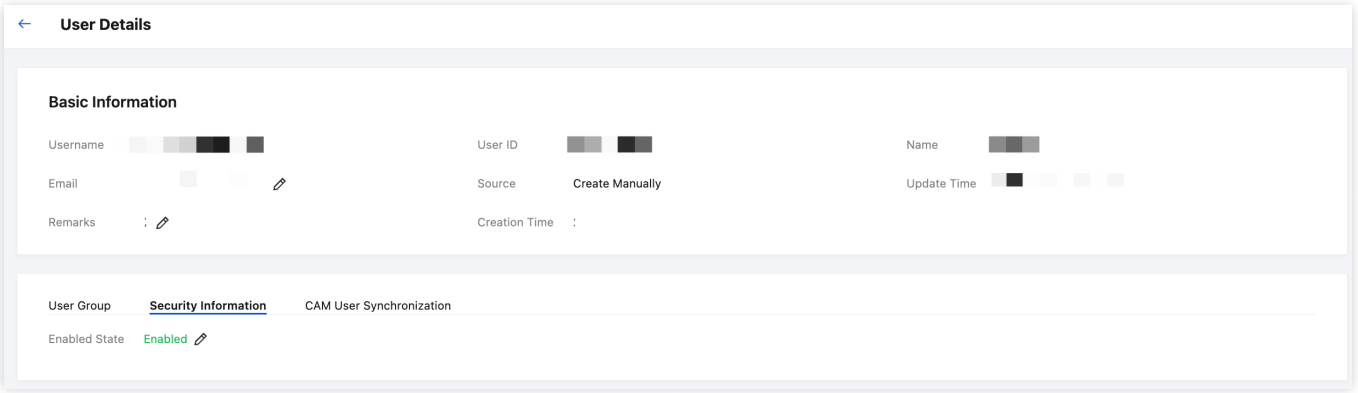
> Note:
>
> Before deleting a user, ensure that the user is not associated with the following resources. Otherwise, the deletion will fail.
>
> - User groups: user groups from which the user will be deleted
> - Permissions: account permissions of the user to be deleted
> - CAM user synchronization: the account synchronization relationship of the user to be deleted

1. In the left sidebar, choose User Management > User.
2. On the User list page, click Delete in the Operation column of the target user.
3. On the Delete User page, click Confirm.

Enabling or Disabling User Login

> Warning:
>
> A user in a disabled state cannot normally log in to the login portal of Identity Center.

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



   - 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.

Managing User Groups

Scenarios

This document introduces the basic operations on user groups, including creating a user group, viewing user group information, modifying basic information of a user group, 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 Cloud Organization > Identity Center.

Operation Steps

Creating a User Group

1. Go to Cloud Organization > Identity Center.
2. In the left sidebar, choose User Management > User Groups.
3. On the user group page, click Create User Group.
4. On the Create User Group panel, enter a user group name.
   The user group name should be unique in the space.
5. Enter the Remark information.
6. Click OK.

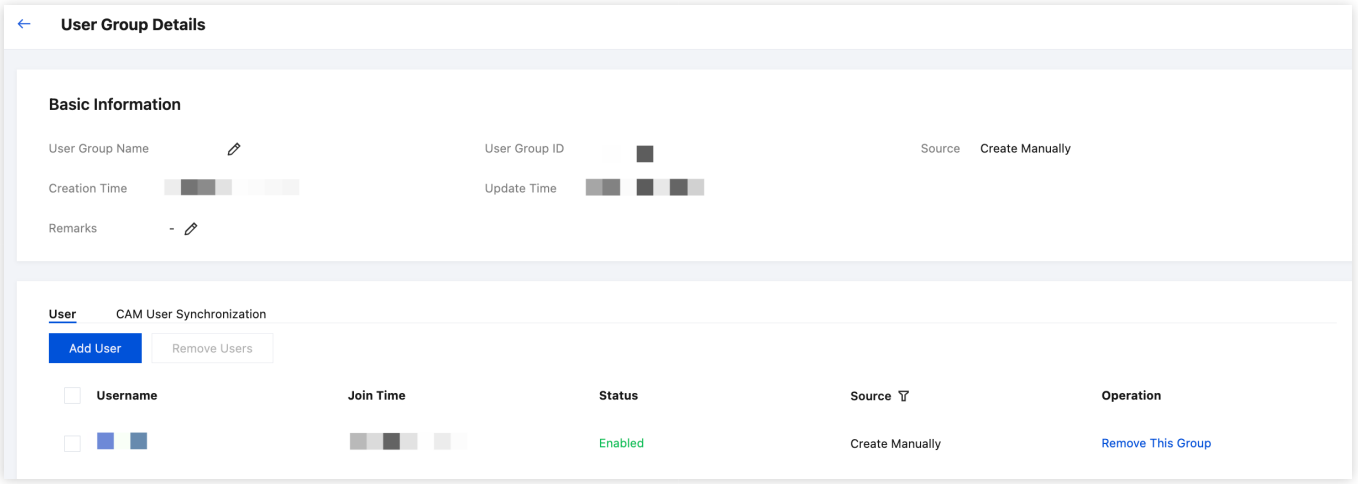
Viewing User Group Information

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

- View basic information of the user group.
- Click the User tab to view users in the user group.
- Click the CAM User Synchronization tab to view the configured CAM user synchronization information.

Modifying the User Group Information

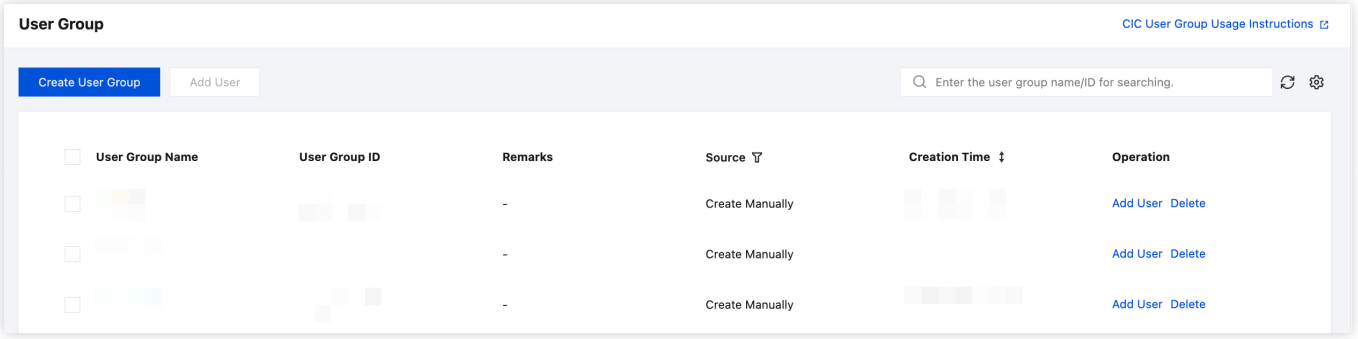
1. On the User Group list page, click the target user group name.
2. In the Basic Info area at the top of the user group details page, the modifiable fields are User Group Name and Remark.



Deleting a User Group

> Note:
>
> Before deleting a user group, ensure that the user group is not associated with the following resources. Otherwise, the deletion will fail.
>
> - Users: users in the use group to be deleted
> - CAM user synchronization: the account synchronization relationship of the user group to be deleted

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



2. In the Delete User Group dialog box, click Confirm.

Adding a User to a User Group

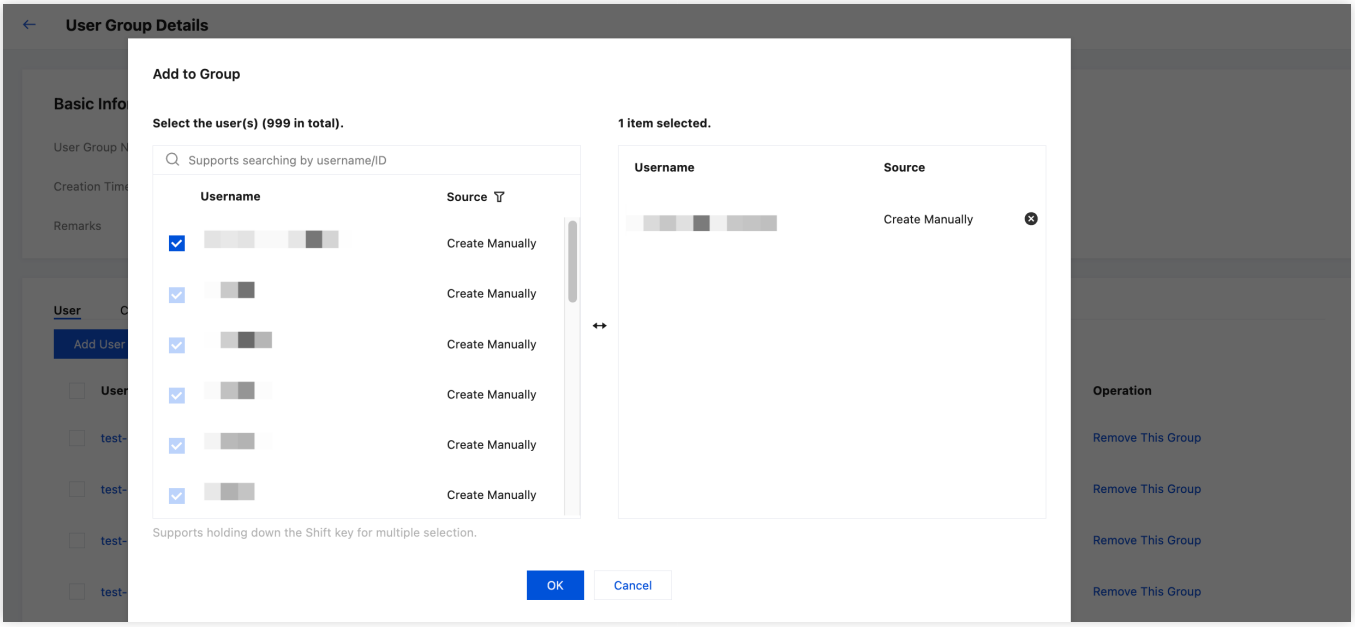
1. On the User Group page, click the target user group name.

2. Click the User tab, and then click Add User.

3. On the Add to Group panel, select users.

> Note:

> A user can be added to multiple user groups.



4. Click OK.

Removing a User from a User Group

1. On the User Group page, click the target user group name.
2. Click the User tab.
3. Click Remove This Group in the Operation column of the target user.
4. In the Remove User dialog box, click Confirm.

Settings
SCIM synchronization
Managing SCIM Keys

Scenarios

A SCIM key is required during SCIM synchronization. This document introduces how to create, disable, enable, and delete a SCIM key.

Use Limits

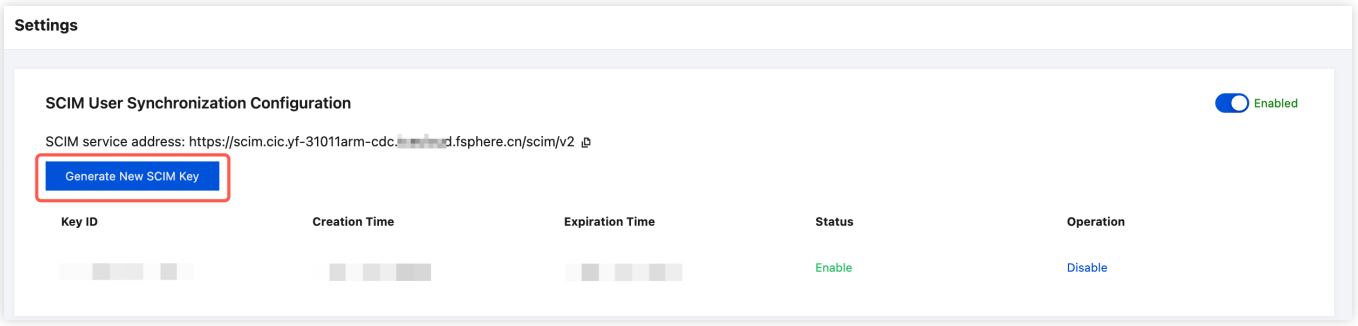
- The SCIM key is displayed only when it is created and cannot be queried. Save it in time.
- A maximum of two SCIM keys can be created.

Creating a SCIM Key

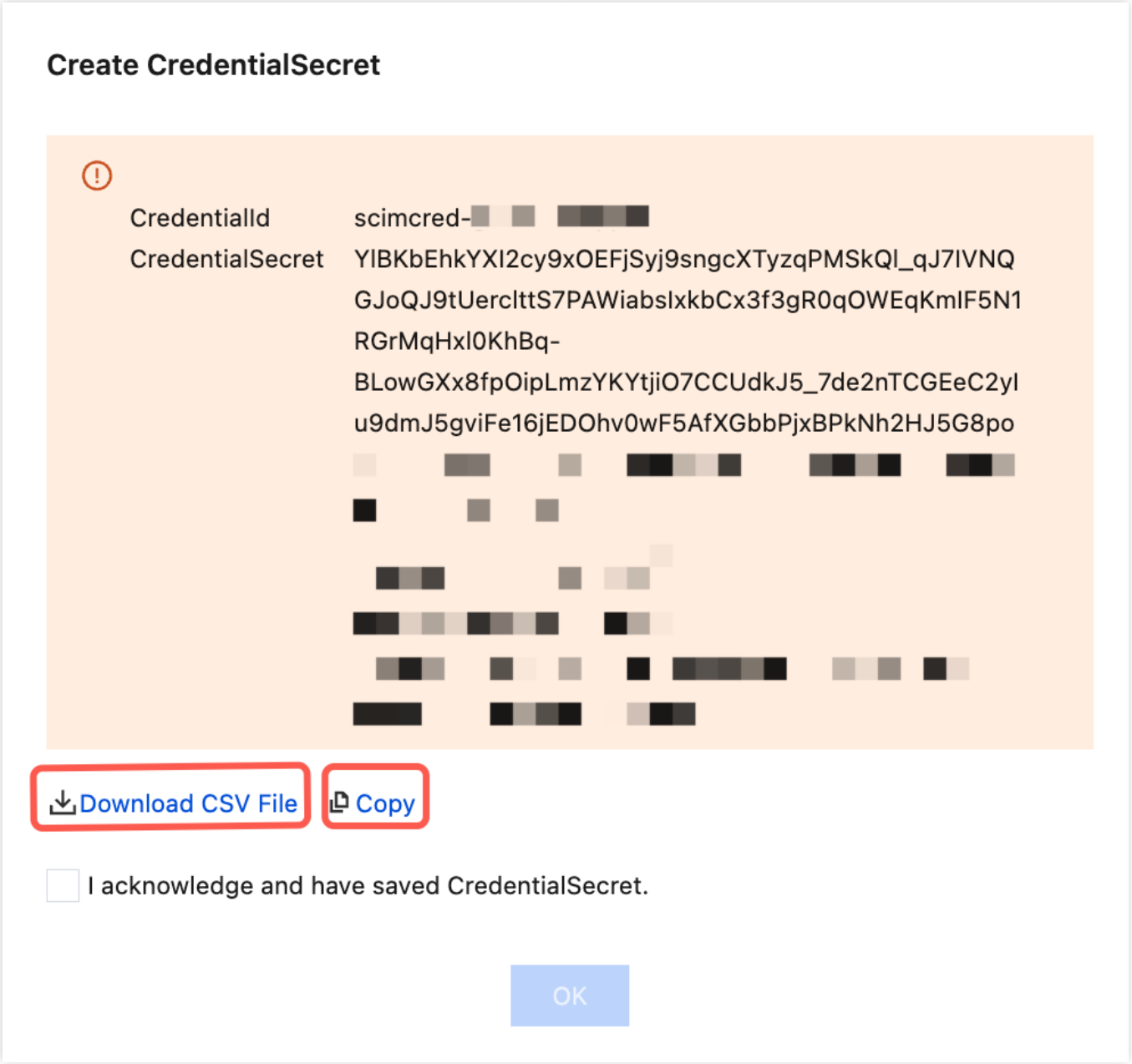
> Note:
>
> A new SCIM key is enabled by default.

1. Log in to Cloud Organization > Identity Center.
2. In the left sidebar, choose User Management > Settings.
3. In the SCIM User Synchronization Configuration area, click Generate New SCIM Key.

   > Note:
   >
   > If you have not enabled SCIM User Synchronization, enable it first.



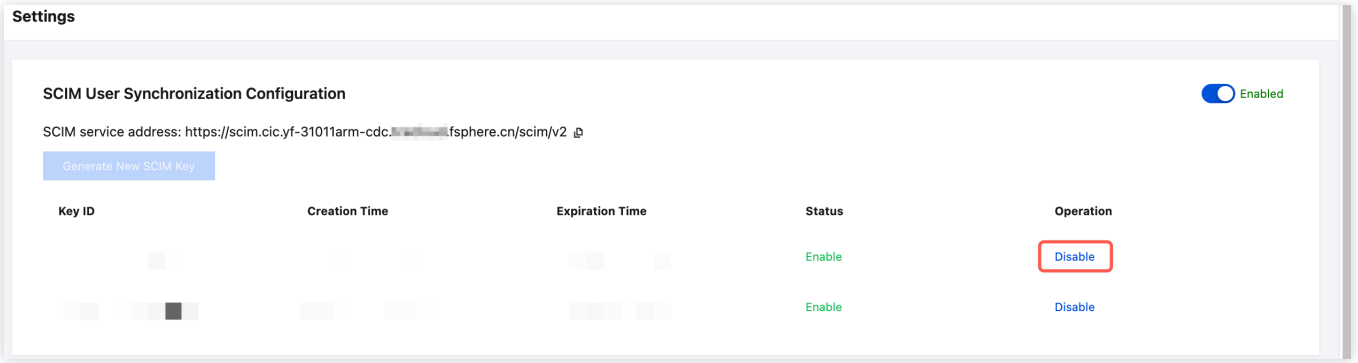
4. In the Create CredentialSecret dialog box, you can save the SCIM key by clicking Download CSV File or Copy. After saving the key, click Confirm.



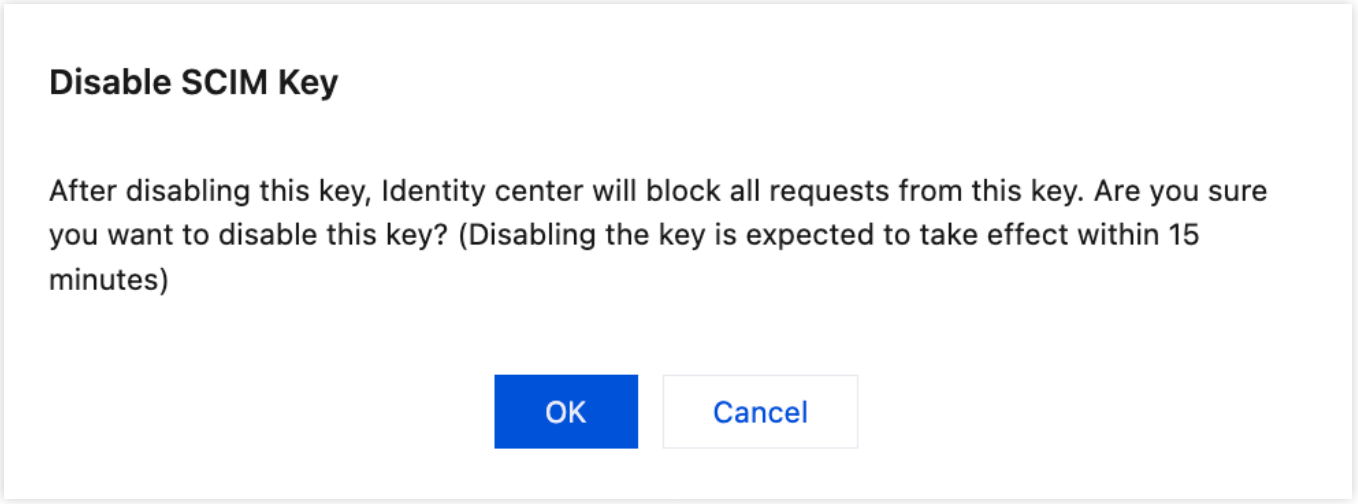
Disabling a SCIM Key

> Warning:
>
> After a SCIM key is disabled, synchronization tasks using the SCIM key will fail.

1. Log in to Cloud Organization > Identity Center.
2. In the left sidebar, choose User Management > Settings.
3. In the SCIM User Synchronization Configuration area, click Disable for the target SCIM key.



4. In the Disable SCIM Key dialog box, click Confirm.



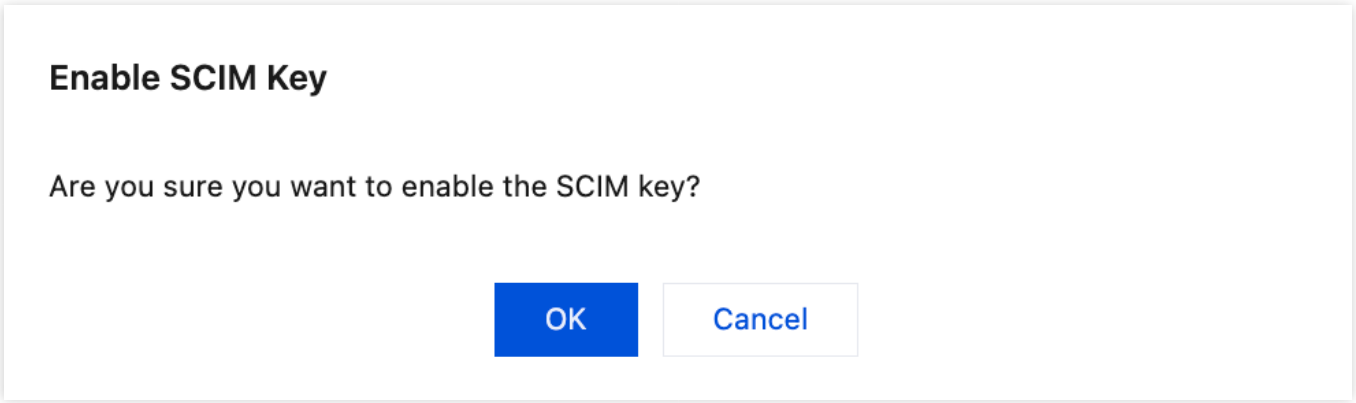
Enabling a SCIM Key

You can re-enable a SCIM key that has been disabled.

1. Log in to Cloud Organization > Identity Center.
2. In the left sidebar, choose User Management > Settings.
3. In the SCIM User Synchronization Configuration area, click Enable for the target SCIM key.



4. In the Enable SCIM Key dialog box, click Confirm.

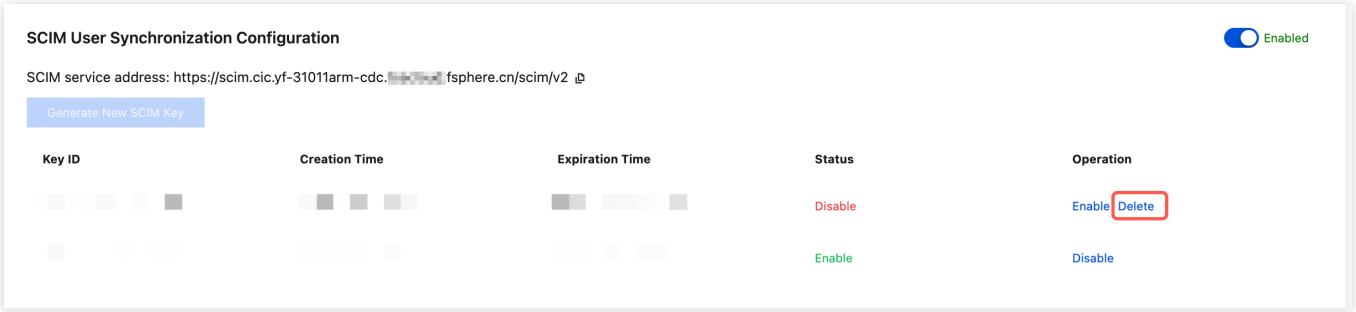


Deleting a SCIM Key

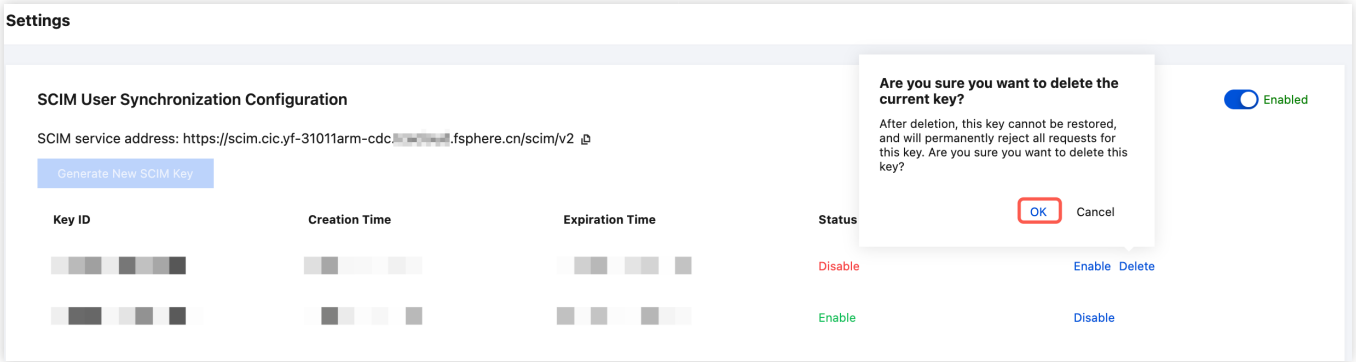
You can delete a SCIM key that is no longer used.

> Warning:
>
> After being deleted, the SCIM key cannot be used anymore.

1. Log in to Cloud Organization > Identity Center.
2. In the left sidebar, choose User Management > Settings.
3. In the SCIM User Synchronization Configuration area, click Delete for the target SCIM key.



4. In the Delete SCIM Key dialog box, click Confirm.



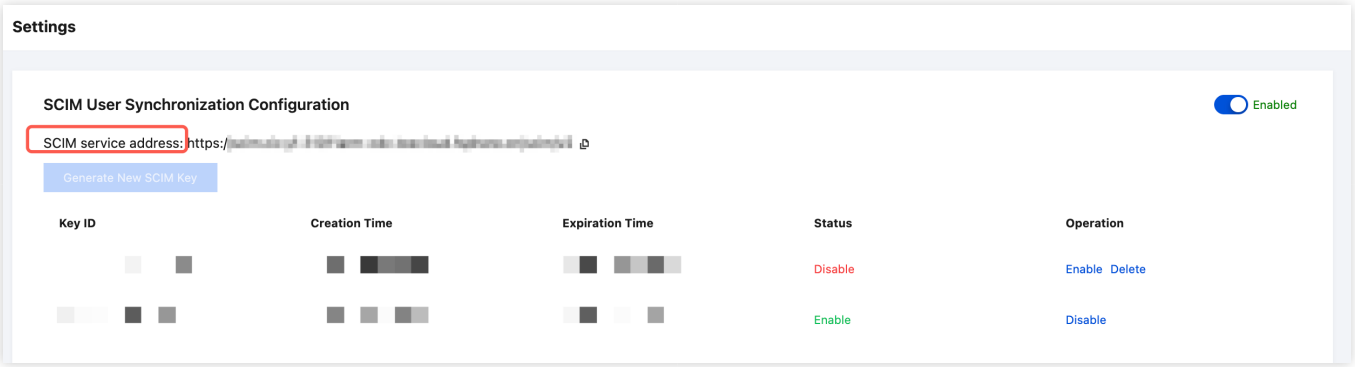
Enabling or Disabling SCIM Synchronization

Scenarios

You can synchronize users or user groups from an external IdP that supports SCIM 2.0 to Identity Center. This document introduces how to obtain the SCIM server address and enable/disable SCIM synchronization.

Obtaining the SCIM Server Address

1. Log in to Cloud Organization > Identity Center.
2. In the left sidebar, choose User Management > Settings.
3. In the SCIM User Synchronization Configuration area, view or copy the SCIM server address, which will be used when SCIM synchronization is configured in the external IdP.



Enabling SCIM Synchronization

After enabling SCIM synchronization, you can synchronize users or user groups from an external IdP to Identity Center. At the same time, you also need to create a SCIM key.

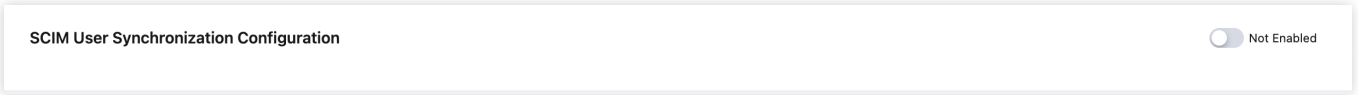
1. Log in to Cloud Organization > Identity Center.

2. In the left sidebar, choose User Management > Settings.

3. In the SCIM User Synchronization Configuration area, click  , and click Enable in the pop-up window to enable SCIM synchronization.

> Note:

> When SCIM is enabled, you cannot modify or delete SCIM users and user groups that have been synchronized to Identity Center, nor can you add or remove users to/from SCIM user groups.



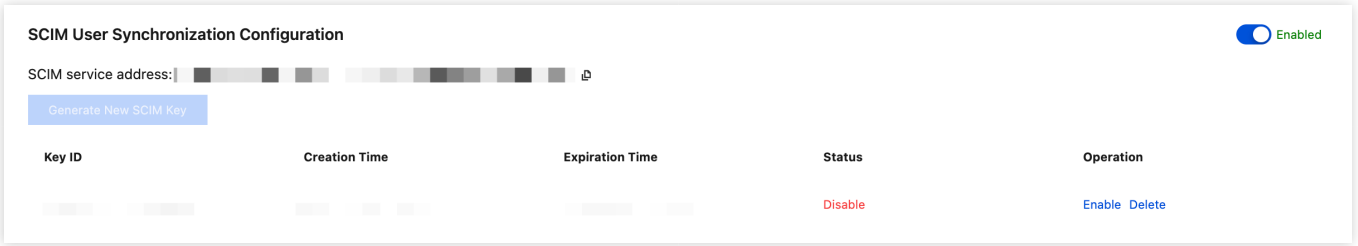
Disabling SCIM Synchronization

The impact of disabling SCIM synchronization is as follows:

- You cannot synchronize users or user groups from an external IdP to Identity Center.
- You can modify or delete SCIM users and user groups that have been synchronized to Identity Center.

> Note:
>
> If you re-enable SCIM synchronization, the attributes of SCIM users or user groups that have been modified in Identity Center may be automatically reverted to their previous values, and SCIM users that have been deleted may be recreated.

1. Log in to Cloud Organization > Identity Center.
2. In the left sidebar, choose User Management > Settings.
3. In the SCIM User Synchronization Configuration area, click  , and click Disable in the pop-up window to disable SCIM synchronization.



SCIM Synchronization Example
Examples of Synchronization from Azure AD via SCIM

This document introduces how to synchronize users or user groups from Azure AD (Azure Active Directory, also known as Microsoft Entra ID) to Identity Center by using the SCIM protocol.

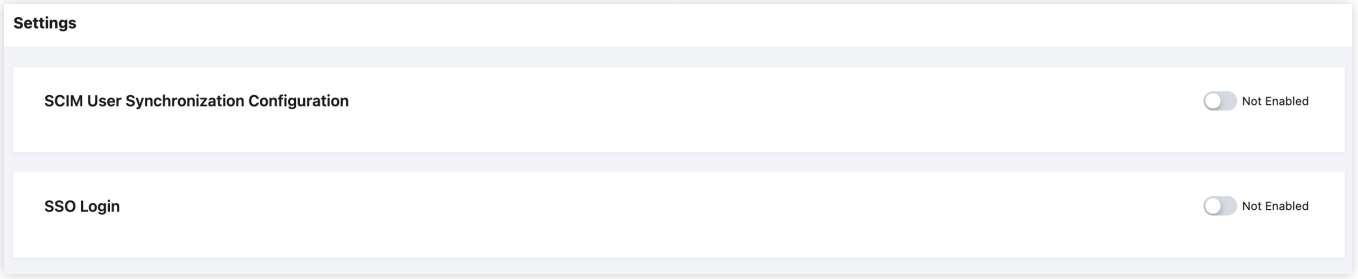
Background Information

All configuration operations in Azure AD need to be performed by an administrator (who has been granted global administrator permissions). For information on how to create a user and authorize the user as an administrator in Azure AD, see Microsoft Entra Documentation.

Configuration in Identity Center

Step 1: Enabling SCIM Synchronization

1. Log in to Cloud Organization > Identity Center.
2. In the left sidebar, choose User Management > Settings.
3. In the SCIM User Synchronization Configuration area, click  , and click Enable in the pop-up window to enable SCIM synchronization.

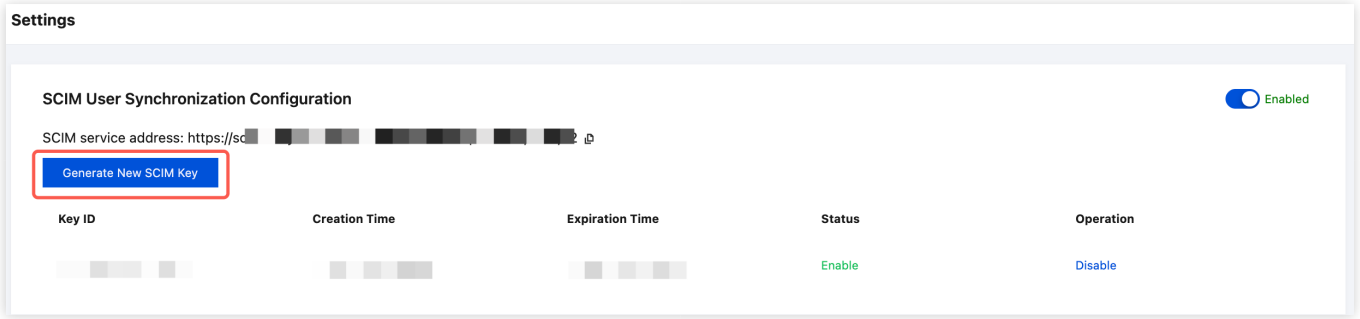


4. After SCIM synchronization is enabled, in the SCIM User Synchronization Configuration area, view or copy the SCIM server address, which will be used when SCIM synchronization is configured in the external IdP.

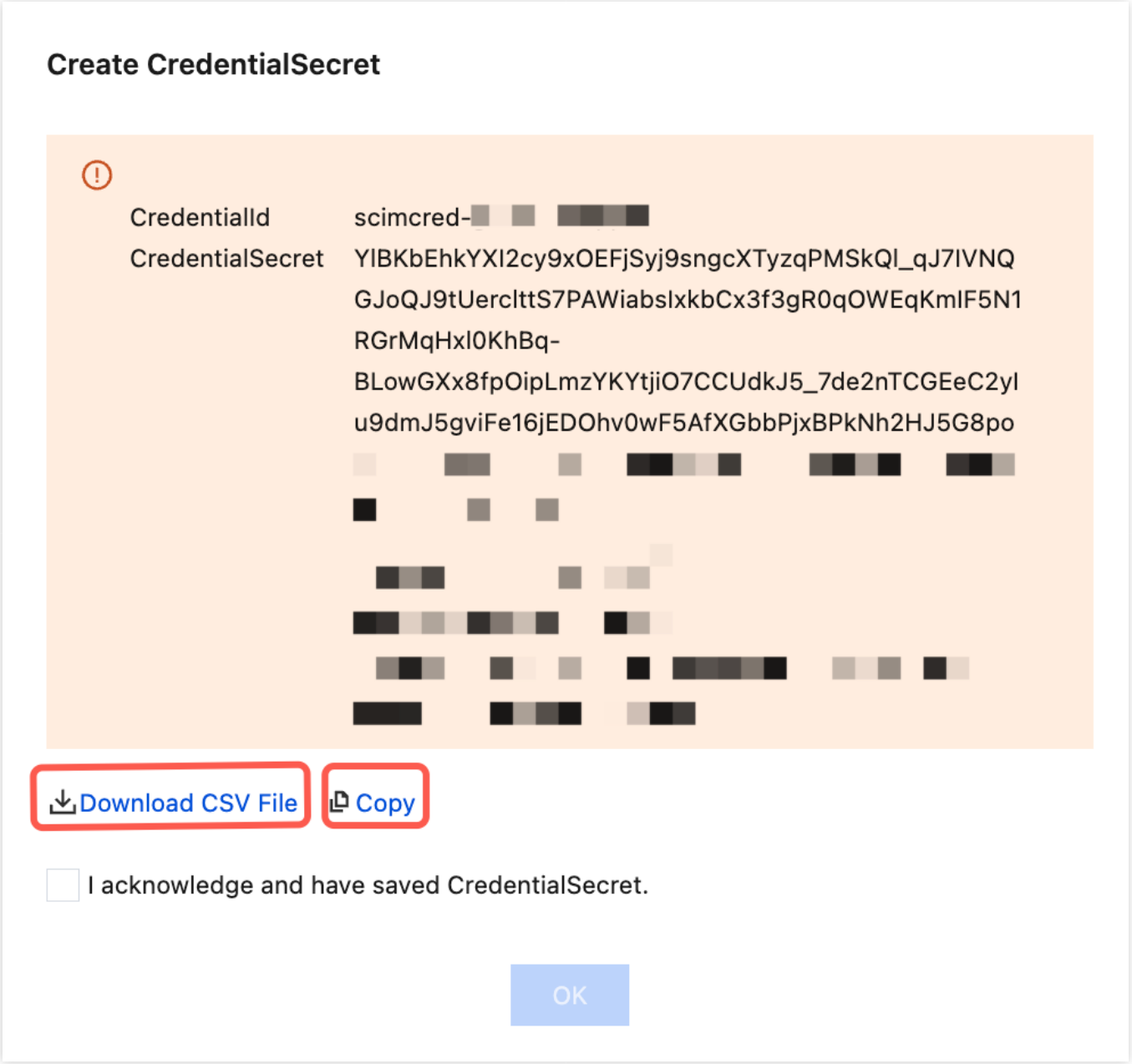


Step 2: Creating a SCIM Key

1. In the SCIM User Synchronization Configuration area, click Generate New SCIM Key.



2. In the Create CredentialSecret dialog box, you can save the SCIM key by clicking Download CSV File or Copy. After saving the key, click Confirm.



Configuration in Azure

Step 1: Creating an Application in Azure AD

1. Log in to the Azure portal as an administrator and click the menu icon in the upper-left corner.

2. In the left sidebar, select Microsoft Entra ID.

3. In the left sidebar, choose Manage > Enterprise Application, and then go to All Applications.

4. Click New Application.

5. On the Browse Microsoft Entra Gallery page, click Create your own application. In the right window, enter an application name (such as SCIM intl), select Integration with any other applications not found in the gallery (Non-gallery), and then click Create.

Step 2: Assigning Users or Groups in Azure AD

1. After creating the application, click Assign Users and Groups in Getting Started.
2. On the Manage > Users and Groups page, click Add User/Group.
3. On the Add Assignment page, select users or user groups and click Select.
4. Click Assign. The successfully assigned users/groups will be displayed in the list.

Step 3: Configuring SCIM Synchronization in Azure AD

1. On the SCIM intl application page, click Provisioning in the left sidebar.

2. On the Provisioning page, click Start.

3. Set the provisioning mode to Auto. In the Admin Credential area, configure the administrator credentials.
   - In the Tenant URL area, enter the SCIM server address.
     Obtain this address from Step 1: Enabling SCIM Synchronization.
   - In the Key Tag area, enter the SCIM key.
     Obtain the SCIM key from Step 2: Creating a SCIM Key.
   - Click Test Connectivity.
     After the test is successful, you can proceed with the next operation.

4. Click Save. The Mapping area appears. You can use the default configuration or modify the attribute mapping as needed.

5. Refresh the page and toggle on the provisioning switch in the Provisioning Status area.

6. ClickSave to complete the configuration.

7. In the provisioning logs of SCIM intl, you can view the synchronization list.

Result Verification

1. Log in to Cloud Organization > Identity Center.
2. In the left sidebar, choose User Management > User/User Group to view the list.
3. The source of synchronized users or user groups will be automatically identified as Import from External Sources.

SCIM 2.0 APIs

If a self-built IdP requires integration with the SCIM protocol to synchronize users or user groups to the User Management module of Identity Center, you need to pay attention to this document. When using the SCIM synchronization capability provided by identity providers such as Okta or Azure AD, you generally do not need to pay attention to this document.

Usage Notes

The implementation of the SCIM 2.0 API follows RFC 7644. For specific requests, see the RFC document.

SCIM API Protocol

Discovery Endpoint

/ServiceProviderConfig

Feature description

- Obtains the features supported by the server side.
  Usage Constraints
- Authentication is not required.
  Request example

```
curl https://scim.convergecloudsso.com/scim/v2/ServiceProviderConfig -H "Content-type:application/json"
```

Response example


```
{
   "authenticationSchemes": [
      {
         "description": "Authentication scheme using the OAuth Bearer Token Standard",
         "documentationUri": "",
         "name": "OAuth Bearer Token",
         "primary": true,
         "specUri": "",
         "type": "oauthbearertoken"
      }
   ],
    "bulk": {
```

```
        "maxOperations": 1000,
        "maxPayloadSize": 1048576,
        "supported": false
    },
    "changePassword": {
        "supported": false
    },
    "documentationUri": "",
    "etag": {
        "supported": false
    },
    "filter": {
        "maxResults": 100,
        "supported": true
    },
    "patch": {
        "supported": true
    },
    "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:ServiceProviderConfig"
    ],
    "sort": {
        "supported": false
    }
}
```


Output:

- Supported features: patch and filter.
- Unsupported features: bulk, changePassword, sort, and etag.

/ResourceTypes

Feature description

- Obtains the resource types supported by the server side. The resource types include User and Group.

  Request example

```
curl https://scim.convergecloudsso.com/scim/v2/ResourceTypes --header 'Authorization: Bearer <your scim credential>' --header "content-type:application/json"
```

Response example


```
{
    "Resources": [
        {
```

```
            "description": "User Account",
            "endpoint": "/Users",
            "id": "User",
            "name": "User",
            "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
            "schemaExtensions": [],
            "schemas": [
                "urn:ietf:params:scim:schemas:core:2.0:ResourceType"
            ]
        },
        {
            "description": "Group",
            "endpoint": "/Groups",
            "id": "Group",
            "name": "Group",
            "schema": "urn:ietf:params:scim:schemas:core:2.0:Group",
            "schemaExtensions": [],
            "schemas": [
                "urn:ietf:params:scim:schemas:core:2.0:ResourceType"
            ]
        }
    ],
    "itemsPerPage": 100,
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "startIndex": 1,
    "totalResults": 2
}
```


/Schemas

Feature description

- Obtains the schemas supported by the server side for User and Group resources.

  Usage Constraints
- Query by resource type is supported.
- Field names and field values in the protocol are case-insensitive.
- Only the fields described in the following text are supported.

  Request example

The schema to request all resources.

```
curl https://scim.convergecloudsso.com/scim/v2/Schemas --header 'Authorization: Bearer <your scim credential>' --header "content-type:application/json"
```

The schema to request users.

curl https://scim.convergecloudsso.com/scim/v2/Schemas/urn:ietf:params:scim:schemas:core:2.0:User --header 'Authorization: Bearer <your scim credential>' --header "content-type:application/json"
The schema to request user groups.
curl https://scim.convergecloudsso.com/scim/v2/Schemas/urn:ietf:params:scim:schemas:core:2.0:Group --header 'Authorization: Bearer <your scim credential>' --header "content-type:application/json"

Response Example

- User Resource Schema


```
{
    "attributes": [
     {
       "caseExact": false,
       "description": "Unique identifier for the User, typically used by the user to directly authenticate to the service provider. Each User MUST include a non-empty userName value. This identifier MUST be unique across the service provider's entire set of Users. REQUIRED.",
       "multiValued": false,
       "mutability": "readWrite",
       "name": "userName",
       "required": true,
       "returned": "default",
       "type": "string",
       "uniqueness": "server"
     },
     {
       "description": "The components of the user's real name. Providers MAY return just the full name as a single string in the formatted sub-attribute, or they MAY return just the individual component attributes using the other sub-attributes, or they MAY return both. If both variants are returned, they SHOULD be describing the same name, with the formatted name indicating how the component attributes should be combined.",
       "multiValued": false,
       "mutability": "readWrite",
       "name": "name",
       "required": false,
       "returned": "default",
       "subAttributes": [
        {
          "caseExact": false,
          "description": "The family name of the User, or last name in most Western languages (e.g., 'Jensen' given the full name 'Ms. Barbara J Jensen, III').",
          "multiValued": false,
          "mutability": "readWrite",
          "name": "familyName",
          "required": false,
          "returned": "default",
```

```
            "type": "string",
            "uniqueness": "none"
          },
          {
            "caseExact": false,
            "description": "The given name of the User, or first name in most Western languages (e.g., 'Barbara' given the full name 'Ms. Barbara J Jensen, III').",
            "multiValued": false,
            "mutability": "readWrite",
            "name": "givenName",
            "required": false,
            "returned": "default",
            "type": "string",
            "uniqueness": "none"
          }
        ],
        "type": "complex"
      },
      {
        "caseExact": false,
        "description": "The name of the User, suitable for display to end-users. The name SHOULD be the full name of the User being described, if known.",
        "multiValued": false,
        "mutability": "readWrite",
        "name": "displayName",
        "required": false,
        "returned": "default",
        "type": "string",
        "uniqueness": "none"
      },
      {
        "description": "A Boolean value indicating the User's administrative status.",
        "multiValued": false,
        "mutability": "readWrite",
        "name": "active",
        "required": false,
        "returned": "default",
        "type": "boolean"
      },
      {
        "description": "Email addresses for the user. The value SHOULD be canonicalized by the service provider, e.g., 'bjensen@example.com' instead of 'bjensen@EXAMPLE.COM'. Canonical type values of 'work', 'home', and 'other'.",
        "multiValued": true,
        "mutability": "readWrite",
        "name": "emails",
        "required": false,
```

```
        "returned": "default",
        "subAttributes": [
         {
          "caseExact": false,
          "description": "Email addresses for the user. The value SHOULD be canonicalized by the service provider, e.g., 'bjensen@example.com' instead of 'bjensen@EXAMPLE.COM'. Canonical type values of 'work', 'home', and 'other'.",
          "multiValued": false,
          "mutability": "readWrite",
          "name": "value",
          "required": false,
          "returned": "default",
          "type": "string",
          "uniqueness": "none"
         },
         {
          "canonicalValues": [
           "work",
           "home",
           "other"
          ],
          "caseExact": false,
          "description": "A label indicating the attribute's function, e.g., 'work' or 'home'.",
          "multiValued": false,
          "mutability": "readWrite",
          "name": "type",
          "required": false,
          "returned": "default",
          "type": "string",
          "uniqueness": "none"
         },
         {
          "description": "A Boolean value indicating the 'primary' or preferred attribute value for this attribute, e.g., the preferred mailing address or primary email address. The primary attribute value 'true' MUST appear no more than once.",
          "multiValued": false,
          "mutability": "readWrite",
          "name": "primary",
          "required": false,
          "returned": "default",
          "type": "boolean"
         }
        ],
        "type": "complex"
       }
      ],
      "description": "User Account",
```

```
    "id": "urn:ietf:params:scim:schemas:core:2.0:User",
    "name": "User",
    "schemas": [
     "urn:ietf:params:scim:schemas:core:2.0:Schema"
    ]
   }
```


- User Group Resource Schema


```
{
    "attributes": [
     {
      "caseExact": false,
      "description": "A human-readable name for the Group. REQUIRED.",
      "multiValued": false,
      "mutability": "readWrite",
      "name": "displayName",
      "required": true,
      "returned": "default",
      "type": "string",
      "uniqueness": "none"
     },
     {
      "description": "A list of members of the Group.",
      "multiValued": true,
      "mutability": "readWrite",
      "name": "members",
      "required": false,
      "returned": "default",
      "subAttributes": [
       {
        "caseExact": false,
        "description": "Identifier of the member of this Group.",
        "multiValued": false,
        "mutability": "immutable",
        "name": "value",
        "required": false,
        "returned": "default",
        "type": "string",
        "uniqueness": "none"
       },
       {
        "caseExact": false,
        "description": "A human-readable name for the group member, primarily used for displa
y purposes.",
```

```
            "multiValued": false,
            "mutability": "immutable",
            "name": "display",
            "required": false,
            "returned": "default",
            "type": "string",
            "uniqueness": "none"
          }
        ],
        "type": "complex"
      }
    ],
    "description": "Group",
    "id": "urn:ietf:params:scim:schemas:core:2.0:Group",
    "name": "Group",
    "schemas": [
      "urn:ietf:params:scim:schemas:core:2.0:Schema"
    ]
  }
```


Users

POST /Users

Feature description

- Synchronizes users.

  Usage Constraints
- If there is a manually created user with the same name in Identity Center, the creation will fail.

  Request example

```
curl https://scim.convergecloudsso.com/scim/v2/Users --header 'Authorization: Bearer <your scim cre
dential>' --header "content-type:application/json" -X POST -d '<data>'
```

The data structure example is as follows:


```
{
    "displayName": "<user display name>",
    "emails": [
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
        }
    ],
```

```
    "name": {
        "familyName": "<user family name>",
        "givenName": "<user given name>"
    },
    "userName": "<user name>"
}
```

Response Example

```
{
    "active": true,
    "displayName": "<user display name>",
    "emails":
    [
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
        }
    ],
    "id": "u-00vrs1l19d6gbsi5****",
    "meta":
    {
        "created": "2023-08-01T13:16:30.000Z",
        "lastModified": "2023-08-01T13:16:30.000Z",
        "resourceType": "User"
    },
    "name":
    {
        "familyName": "<user family name>",
        "givenName": "<user given name>"
    },
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "userName": "<user name>"
}
```

GET /Users/{id} and GET /Users

Feature description

- GET /Users/{id}: queries users with specified IDs.
- GET /Users: queries user information by condition, or queries a list of all users.

  Usage Constraints

- If /{id} is included, the user with that ID is returned. If {id} does not correspond to an existing user, the request is rejected.
- If /{id} is not included and a filter is available, the corresponding user is filtered and returned. The filter only supports the userName field and the eq operator.
- If /{id} is not included and no filter is available, a list of all users is returned. The standard pagination method of the SCIM protocol is supported. A maximum of 100 records can be returned per page. If the number of records exceeds 100 (count > 100), the response is limited to 100 records per page.
- Only synchronized users can be queried.

1. Example 1: Query users with specified IDs.
   Request example

```
curl https://scim.convergecloudsso.com/scim/v2/Users/<userId> --header 'Authorization: Beare
r <your scim credential>' --header "content-type:application/json" -X GET
```

   Response example

```
{
    "active": true,
    "displayName": "<user display name>",
    "emails":
    [
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
        }
    ],
    "id": "u-00vrs1l19d6gbsi5****",
    "meta":
    {
        "created": "2023-08-01T13:16:30.000Z",
        "lastModified": "2023-08-01T13:16:30.000Z",
        "resourceType": "User"
    },
    "name":
    {
        "familyName": "<user family name>",
        "givenName": "<user given name>"
    },
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:User"
```

```
    ],
    "userName": "<user name>"
}
```

2. Example 2: Query user information by condition, or query a list of all users.
   Request example

```
curl https://scim.convergecloudsso.com/scim/v2/Users<?parameters> --header 'Authorizatio
n: Bearer <your scim credential>' --header "content-type:application/json" -X GET
```

   Response example
   GET /Users?filter=userName eq "Test_User"

```
{
    "Resources":
    [
        {
            "active": true,
            "displayName": "<user display name>",
            "emails":
            [
                {
                    "primary": true,
                    "type": "work",
                    "value": "<user email>"
                }
            ],
            "id": "u-0015b4962vrywtzb****",
            "meta":
            {
                "created": "2023-07-07T17:21:07.000Z",
                "lastModified": "2023-07-07T17:21:07.000Z",
                "resourceType": "User"
            },
            "name":
            {
                "familyName": "<user family name>",
                "givenName": "<user given name>"
            },
            "schemas":
            [
                "urn:ietf:params:scim:schemas:core:2.0:User"
            ],
            "userName": "<user name>"
```

```
        },
        {
            "active": true,
            "displayName": "<user display name>",
            "emails":
            [
                {
                    "primary": true,
                    "type": "work",
                    "value": "<user email>"
                }
            ],
            "id": "u-00vrs1l19d6gbsi5****",
            "meta":
            {
                "created": "2023-08-01T13:16:30.000Z",
                "lastModified": "2023-08-01T13:16:30.000Z",
                "resourceType": "User"
            },
            "name":
            {
                "familyName": "<user family name>",
                "givenName": "<user given name>"
            },
            "schemas":
            [
                "urn:ietf:params:scim:schemas:core:2.0:User"
            ],
            "userName": "<user name>"
        }
    ],
    "itemsPerPage": 10,
    "schemas":
    [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "startIndex": 1,
    "totalResults": 2
}


{
    "Resources": [],
    "itemsPerPage": 10,
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
```

```
    "startIndex": 1,
    "totalResults": 0
}
```


PUT /Users/{id} and PATCH /Users/{id}

Description

- PUT /Users/{id}: replaces user information.
- PATCH /Users/{id}: updates user information.

Usage Constraints

- {id} is required. The fields that can be modified are limited to those defined in the schema.
- PUT overwrites original attributes.
- Patch supports Add and Replace.
- Only synchronized users can be modified.

Request example

1. Replace user information (PUT).

```
curl https://scim.convergecloudsso.com/scim/v2/Users/<userId> --header 'Authorization: Beare
r <your scim credential>' --header "content-type:application/json" -X PUT -d '<data>'
```

The data structure example is as follows:


```
 {
   "active": false,
   "displayName": "<user display name>",
   "emails":
   [
      {
         "primary": true,
         "type": "work",
         "value": "<user email>"
      }
   ],
   "name":
   {
      "familyName": "<user family name>",
      "givenName": "<user given name>"
   },
   "userName": "<user name>"
}
```

2. Update user information (PATCH).

curl https://scim.convergecloudsso.com/scim/v2/Users/<userId> --header 'Authorization: Beare r <your scim credential>' --header "content-type:application/json" -X PATCH -d '<data>'

The data structure example is as follows:

```
// Replace operations
{
   "Operations": [
      {
         "op": "replace",
         "path": "",
         "value": {
            "active": false,
            "displayName": "displayName",
            "name": {
               "familyName": "familyName",
               "givenName": "givenName"
            }
         }
      }
   ],
   "schemas": [
      "urn:ietf:params:scim:api:messages:2.0:PatchOp"
   ]
}
// Add operations
{
   "Operations": [
      {
         "op": "add",
         "path": "",
         "value": {
            "displayName": "displayName",
            "name": {
               "familyName": "familyName",
               "givenName": "givenName"
            }
         }
      },
      {
         "op": "add",
         "path": "active",
         "value": true
```

```
            }
        ],
        "schemas": [
            "urn:ietf:params:scim:api:messages:2.0:PatchOp"
        ]
    }
```

Response example

```
//replace
{
    "active": false,
    "displayName": "displayName",
    "emails":
    [
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
        }
    ],
    "id": "u-00vrs1l19d6gbsi5****",
    "meta":
    {
        "created": "2023-08-01T13:16:30.000Z",
        "lastModified": "2023-08-01T13:16:30.000Z",
        "resourceType": "User"
    },
    "name":
    {
        "familyName": "<user family name>",
        "givenName": "<user given name>"
    },
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "userName": "<user name>"
}

//add
{
    "active": true,
    "displayName": "displayName",
    "emails":
```

```
    [
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
        }
    ],
    "id": "u-00vrs1l19d6gbsi5****",
    "meta":
    {
        "created": "2023-08-01T13:16:30.000Z",
        "lastModified": "2023-08-01T13:16:30.000Z",
        "resourceType": "User"
    },
    "name":
    {
        "familyName": "<user family name>",
        "givenName": "<user given name>"
    },
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "userName": "<user name>"
}
```


DELETE /Users/{id}

Feature description

- Deletes users with specified IDs.

  Usage Constraints
- {id} is required.
- Only synchronized users can be deleted.

  Request example

```
curl https://scim.convergecloudsso.com/scim/v2/Users/<userId> --header 'Authorization: Bearer <your scim credential>' --header "content-type:application/json" -X DELETE
```

Response example

```
HTTP/1.1 204
Date: Tue, 31 Mar 2020 02:36:15 GMT
Content-Type: application/json
x-RequestId: abbf9e53-9ecc-46d2-8efe-104a66ff128f
```

/Group

POST /Groups

Feature description

- Synchronizes user groups.

  Usage Constraints
- If there is a manually created user group with the same name in Identity Center, the creation will fail.

  Request example

```
curl https://scim.convergecloudsso.com/scim/v2/Groups --header 'Authorization: Bearer <your scim cr
edential>' --header "content-type:application/json" -X POST -d '<data>'
```

The data structure example is as follows:

```
{
   "displayName": "<group name>",
   "schemas": [
      "urn:ietf:params:scim:schemas:core:2.0:Group"
   ]
}
```

Response example

```
{
   "displayName": "<group name>",
   "id": "g-00nqnd7hoevd1unv****",
   "members": [],
   "meta":
   {
      "created": "2023-08-01T13:30:23.000Z",
      "lastModified": "2023-08-01T13:30:23.000Z",
      "resourceType": "Group"
   },
   "schemas":
   [
      "urn:ietf:params:scim:schemas:core:2.0:Group"
   ]
```

}

GET /Groups/{id} and GET /Groups

Feature description

- GET /Groups/{id}: queries user groups with specified IDs.
- GET /Groups: queries user group information by condition, or queries a list of all user groups.
  Usage Constraints
- Information can be queried by ID and filter criteria.
- The filter only supports the displayName field and the eq operator.
- If /{id} is included, the user group with that ID is returned, and parameter values of members are included. If {id} does not correspond to an existing user, the request is rejected.
- If /{id} is not included and no filter is available, a list of all user groups is returned, and values of members are empty. The list method does not return members. The standard pagination method of the SCIM protocol is supported. A maximum of 100 records can be returned. If the number of records exceeds 100 (count > 100), the response is limited to 100 records per page.
- Only synchronized user groups can be queried.

1. Example 1: Query user groups with specified IDs.
   Request example

```
curl https://scim.convergecloudsso.com/scim/v2/Groups/<groupId> --header 'Authorization: B
earer <your scim credential>' --header "content-type:application/json" -X GET
```

   Response example

```
{
  "displayName": "<group name>",
  "id": "g-00nqnd7hoevd1unv****",
  "members":
  [
     {
        "display": "xxx",
        "value": "u-00vrs1l19d6gbsi5****"
     }
  ],
  "meta":
  {
     "created": "2023-08-01T13:30:23.000Z",
     "lastModified": "2023-08-01T13:30:23.000Z",
     "resourceType": "Group"
  },
```

```
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:Group"
    ]
}
```

2. Example 2: Query user group information by condition, or query a list of all user groups.
   Request example

```
curl https://scim.convergecloudsso.com/scim/v2/Groups<?parameters> --header 'Authorizatio
n: Bearer <your scim credential>' --header "content-type:application/json" -X GET
```

   Response example

```
{
    "Resources":
    [
        {
            "displayName": "<group name>",
            "id": "g-00nqnd7hoevd1unv****",
            "members": [],
            "meta":
            {
                "created": "2023-08-01T13:30:23.000Z",
                "lastModified": "2023-08-01T13:30:23.000Z",
                "resourceType": "Group"
            },
            "schemas":
            [
                "urn:ietf:params:scim:schemas:core:2.0:Group"
            ]
        }
    ],
    "itemsPerPage": 10,
    "schemas":
    [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "startIndex": 1,
    "totalResults": 1
}
```

PUT /Groups/{id} and PATCH /Groups/{id}

Feature description

- PUT /Groups/{id}: replaces user group information.
- PATCH /Groups/{id}: updates user group information.
  Usage Constraints
- {id} is required. The fields that can be modified are limited to those defined in the schema.
- PUT overwrites original attributes and supports member replacement.
- Patch supports Add, Replace, and Remove.
- Only synchronized user groups can be modified.
  Request example
- Replace user group information (PUT).

  curl https://scim.convergecloudsso.com/scim/v2/Groups/<groupId> --header 'Authorization: Bearer <your scim credential>' --header "content-type:application/json" -X PUT -d '<data>'

  The data structure example is as follows:

  ```
  {
     "displayName": "<group name>",
     "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:Group"
     ]
  }
  ```

- Update user group information (PATCH).

  curl https://scim.convergecloudsso.com/scim/v2/Groups/<groupId> --header 'Authorization: Bearer <your scim credential>' --header "content-type:application/json" -X PATCH -d '<data>'

  The data structure example is as follows:

  ```
  //Remove the specified user <userId> from the group corresponding to <groupId>.
  {
     "Operations": [
  ```

```
        {
            "op": "remove",
            "path": "members",
            "value": [
                {
                    "value": "<userId>"
                }
            ]
        }
    ],
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:PatchOp"
    ]
}
//Remove all users from the group corresponding to <groupId>.
{
    "Operations": [
        {
            "op": "remove",
            "path": "members"
        }
    ],
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:PatchOp"
    ]
}
//Add three users to the group corresponding to <groupId>.
{
    "Operations": [
        {
            "op": "add",
            "path": "members",
            "value": [
                {
                    "display": "<userName1>",
                    "value": "<userId1>"
                },
                {
                    "display": "<userName2>",
                    "value": "<userId2>"
                },
                {
                    "display": "<userName3>",
                    "value": "<userId3>"
                }
            ]
        }
```

```
    ],
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:PatchOp"
    ]
}
```

Response Example

```
HTTP/1.1 204 No Content
HTTP/1.1 204
Date: Tue, 07 Apr 2020 23:59:09 GMT
Content-Type: application/json
x-RequestId: dad0c91c-1ea8-4b36-9fdb-4f099b59c1c9
```

DELETE /Groups/{id}

Feature description

- Deletes user groups with specified IDs.

  Usage Constraints
- {id} is required.
- A group with members cannot be deleted.
- Only synchronized user groups can be deleted.

  Request example

```
curl https://scim.convergecloudsso.com/scim/v2/Groups/<groupId> --header 'Authorization: Bearer <
your scim credential>' --header "content-type:application/json" -X DELETE
```

Response Example

```
HTTP/1.1 204
Date: Mon, 06 Apr 2020 22:21:24 GMT
Content-Type: application/json
x-RequestId: abbf9e53-9ecc-46d2-8efe-104a66ff128
```

Managing SSO

Scenarios

Identity Center of Cloud Organization supports SSO based on SAML 2.0. The cloud platform is an SP, and the identity management system of an enterprise is an IdP. Through SSO, enterprise employees can use users in the IdP to log in to Identity Center directly.

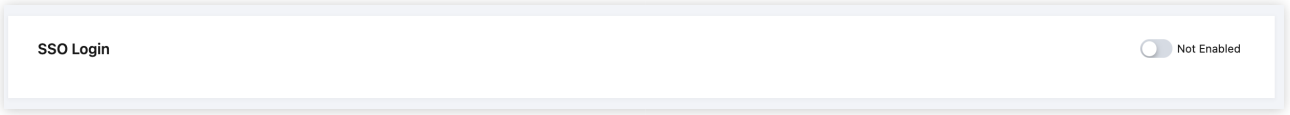
Operation Steps

Enabling SSO

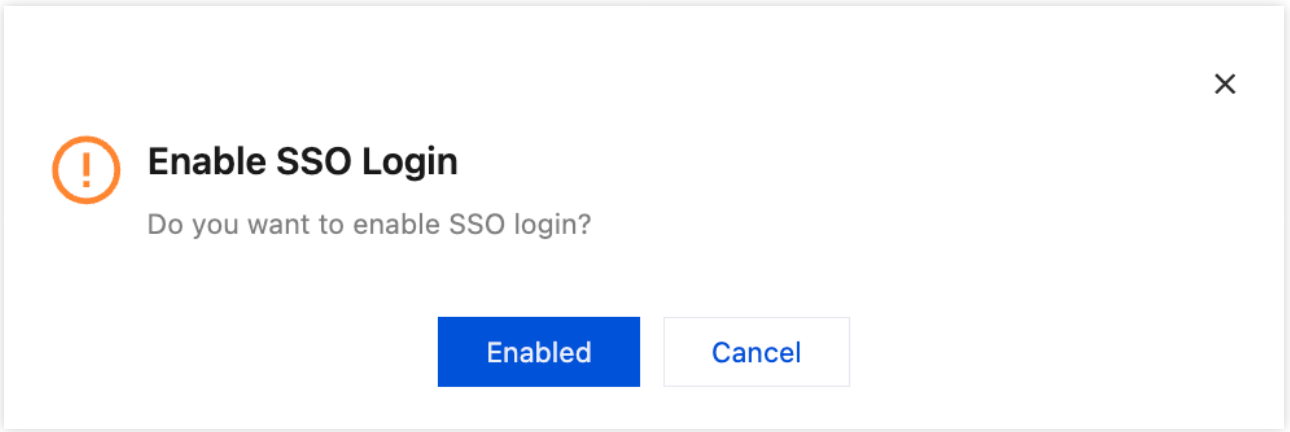
1.Log in to the Cloud Organization console and choose Identity Center Management > Settings **>**SSO Login. After enabling SSO, you can configure IdP information.

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

1. In the SSO Login area, toggle on the SSO switch.

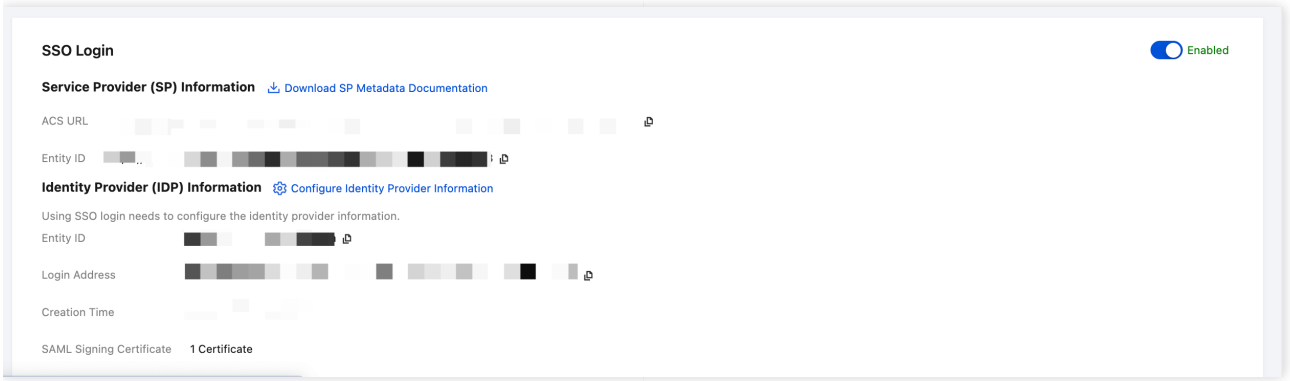


2. In the Enable SSO Login dialog box, click Enable.



Managing SP Information

When configuring SSO in an external IdP, you need to use the SP metadata file. You can download this file by performing the following operations: Log in to the Cloud Organization console, choose Identity Center Management > Settings **>**SSO Login, and click Download SP Metadata Document in the Service Provider (SP) Info area. You can also view or copy the ACS URL and Entity ID information for manual configuration in an external IdP.



Managing IdP Information

You need to configure IdP information and toggle on the SSO switch to use the SSO feature normally.
Both manual configuration and metadata file upload are supported to configure IdP information.

- Manual configuration only applies to 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 IdP Information

You need to configure IdP information before enabling SSO.

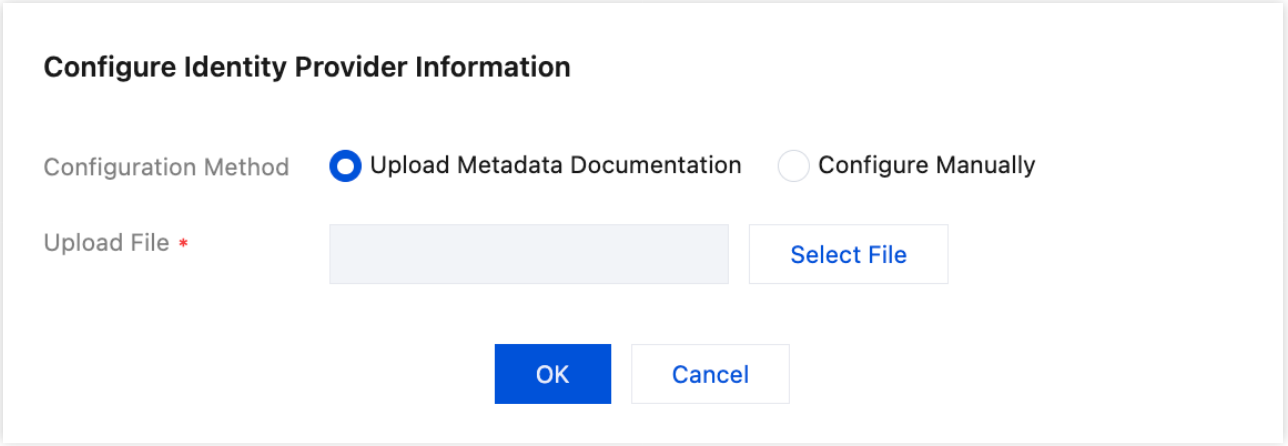
1. You have logged in to Cloud Organization > Identity Center.

2. In the left sidebar, click Settings.

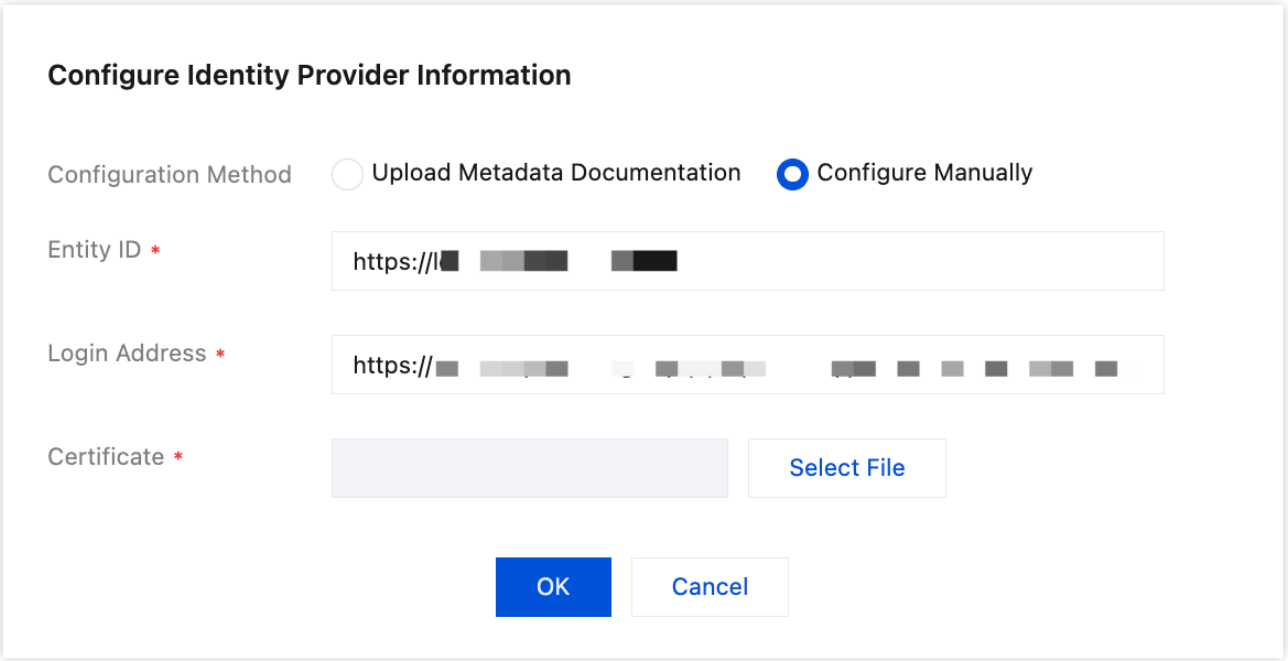
3. In the Identity Provider (IdP) Information area of SSO Login, click Configure Identity Provider Information.

4. In the Configure Identity Provider Information dialog box, select Upload Metadata Documentation or Manual Configuration to configure IdP information.
   You can choose either of the following two methods for configuration. Obtain the relevant metadata file or configuration information from your IdP.

   - Upload the metadata file
     Click Select File to upload the IdP's metadata file.



- Manual configuration



  - Entity ID: IdP identifier.
  - Login Address: IdP login address.
  - Certificate: a certificate used by the IdP for SAML response signing. You can click Select a File to upload the IdP's certificate.

5. Click OK.

Updating IdP Information

You can update IdP information regardless of whether SSO is enabled or disabled. However, when you update the information when SSO is enabled, inconsistencies between new and existing IdP information may cause SSO failure. Proceed with caution.

1. In the Identity Provider (IdP) Information area of SSO Login, 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.

Managing Multi-Account Authorization
Multi-account Authorization Overview

On the Multi-account Authorization page, you can configure CAM user synchronization according to the directory structure of your cloud organization.

Identity Center users can access the account's cloud resources through CAM users. Detailed descriptions are as follows:

Access Method	Note	Synchronization Method
Configuring CAM User Synchronization	Enterprises manage users accessing the cloud platform in Cloud Organization 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 accounts.	When configuring CAM user synchronization, 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.

CAM User Synchronization Description

If you need to perform a one-time batch authorization for multiple accounts and multiple identities, you can choose Cloud Organization > Identity Center, go to 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.
2. Select one or more Identity Center identities.
3. Click Configure CAM User Synchronization. The Identity Center service will complete the authorization for you in batches.
    - In batch synchronization, if a duplicate operation is attempted for some existing synchronizations, the operation will fail. However, new 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 permissions on 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.

Configuring CAM Role Synchronization

Scenarios

According to the cloud organization structure, you can set users or user groups with access permissions for each account and configure their permissions.
This section provides an example of how to deploy the permission configuration on a member account (Account1) for an Identity Center user (user1). The permission configuration only defines permissions to access Cloud Virtual Machine (CVM), allowing the Identity Center user (user1) to access only the CVM resources of the member account (Account1).

Prerequisites

Please ensure that you have created the permission configuration.
The permission configuration used in this example has already been bound to a preset policy. No custom policy needs to be created.
Please ensure that you have created or synchronized users.
The user (user1) created in Identity Center is used in this example. For detailed operations, see Managing Users.

Managing CAM User Synchronization
Configuring CAM User Synchronization

Scenarios

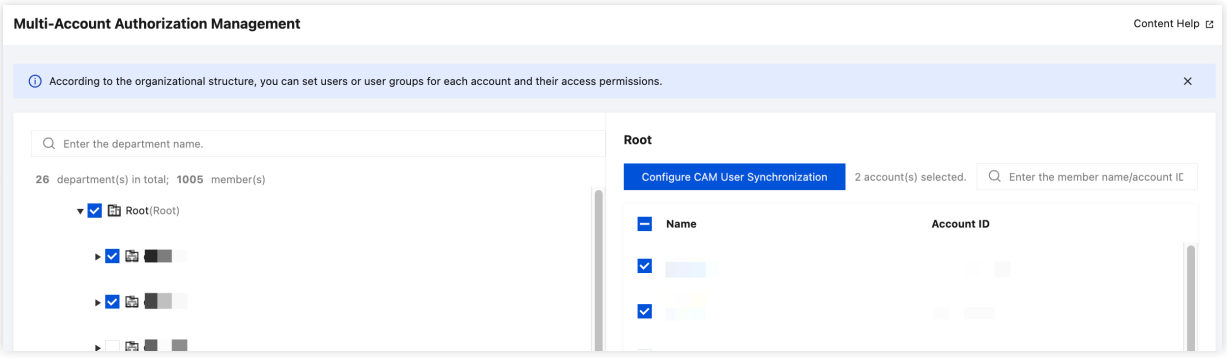
You can configure CAM user synchronization, create a CAM user with the same name as the Identity Center user in the target account, and then access resources in the account via the CAM user.
This document provides an example on how to configure CAM user synchronization, create a CAM user (user1) with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

Operation Steps

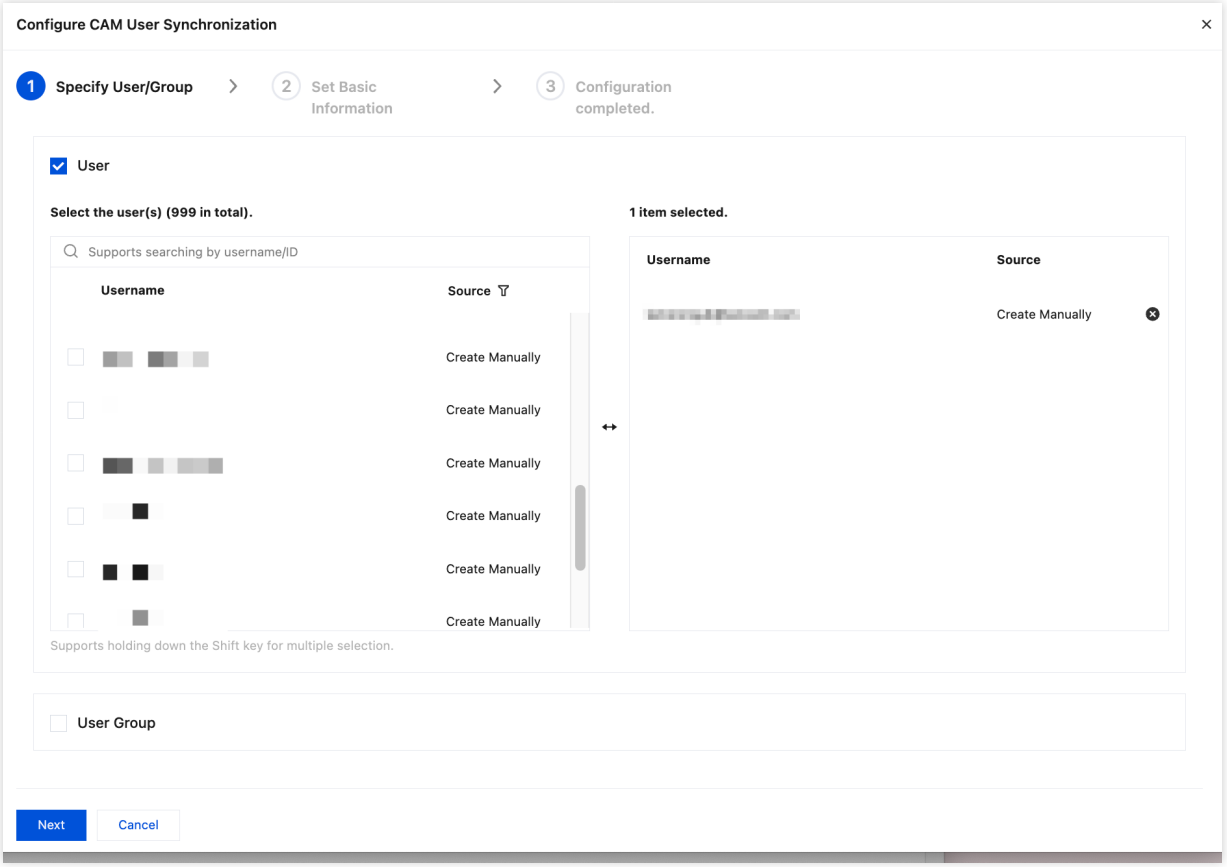
Step 1: Configuring CAM User Synchronization

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

1. Choose **Cloud Organization >**Identity Center.
2. In the left sidebar, click CAM Sync > Multi-account Authorization Management.
3. On the Multi-account Authorization Management page, select a target account.
   In this example, a member account (Account1) is selected.
4. Click Configure CAM User Synchronization.

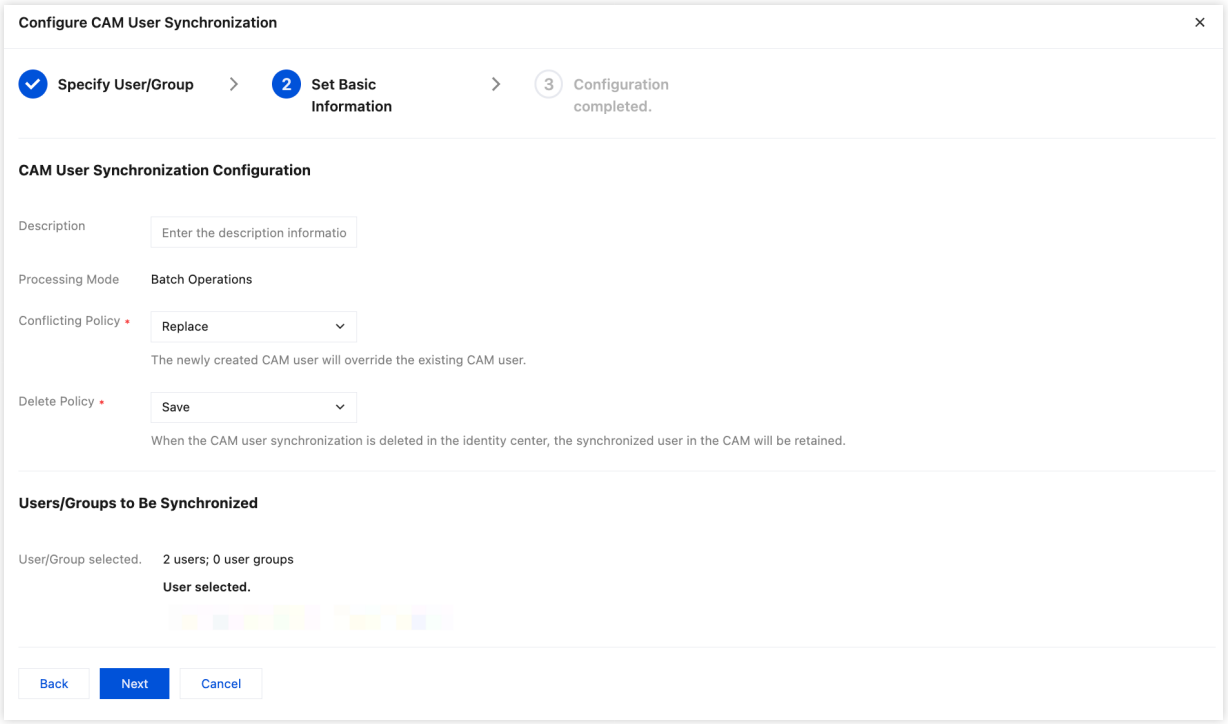


5. On the Configure CAM User Synchronization panel, select a target user or user group, and click Next.
   In this example, an Identity Center user (user1) is selected.



6. Set the following basic information, and then click Next.
   i. Enter a description of CAM user synchronization.
   ii. Configure Conflict Policy.
   - Conflict policy: a policy to handle the situation where a CAM user with the same name exists in the target account.
     - Replace: The created CAM user will overwrite the existing CAM user.
     - Save Both: The created CAM user will be renamed by the system, and both the new and old CAM users will be retained.

   iii. Configure Deletion Policy.
   - Deletion policy: the handling policy for already synchronized CAM users when the CAM user synchronization is deleted.
     - Retain: When the CAM user synchronization is deleted, the already synchronized CAM user will be retained.
     - Delete: When the CAM user synchronization is deleted, the already synchronized CAM user will be deleted.



7. Click Complete.
   After successful configuration, a CAM user with the same name will be created in the target account. In this example, a CAM user (user1) 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

Sub-users synchronized to CAM through Identity Center > Configure CAM User Synchronization are not granted any permission. You need to authorize these users in the CAM console. If you need to preset permissions through Identity Center, choose to configure CAM role synchronization.

1. Log in to the member account (Account1).
2. Authorize the CAM user (user1).
   In this example, the CAM user (user1) will be granted administrative permissions for CVM. For specific operations, see Sub-user Permission Settings.

Step 3: Accessing the Cloud Platform as an Identity Center User

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

1. Log in to the Identity Center user portal as an Identity Center user (user1).
   For specific operations, see Identity Center User Login.
2. Access CVM resources in the member account (Account1) as a CAM user.

Viewing/Modifying/Deleting User Synchronization

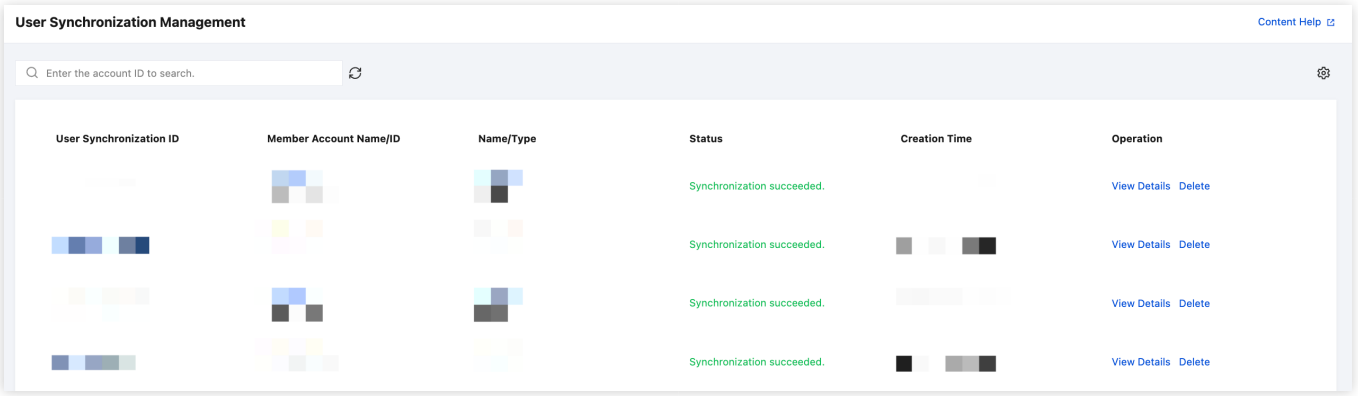
Scenarios

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

Operation Steps

Viewing CAM User Synchronization

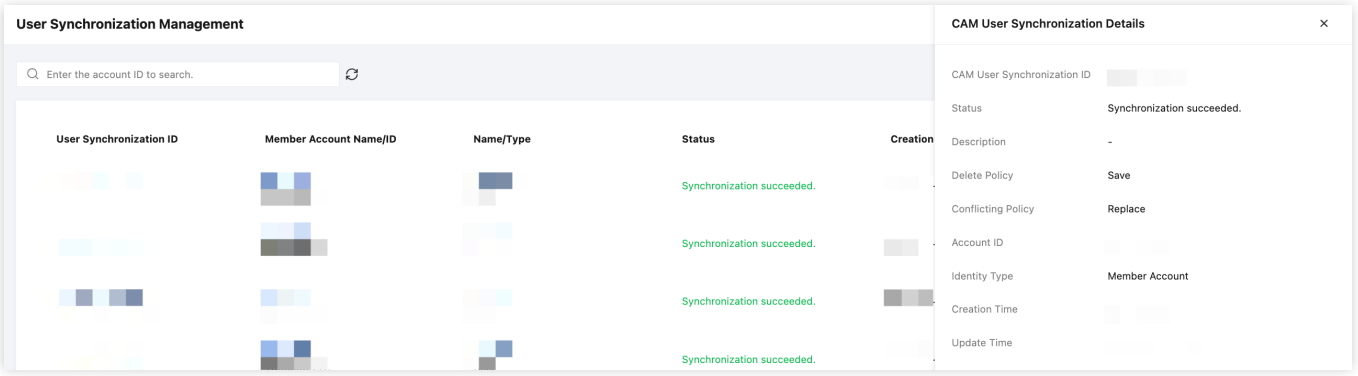
1. Go to Cloud Organization > Identity Center.
2. In the left sidebar, choose CAM Synchronization > User Synchronization Management.



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

Modifying CAM User Synchronization

1. Go to Cloud Organization > Identity Center.
2. In the left sidebar, choose CAM Synchronization > User Synchronization Management.
3. On the User Synchronization Management page, click View Detail in the Operation column of the target user synchronization.
4. On the User Synchronization Detail panel, click Edit to modify the description or deletion policy.
   For the meaning of configuration items, see Configuring CAM User Synchronization.



Deleting CAM User Synchronization

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

User Login
Identity Center User Login

Scenarios

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 users.

Operation Steps

Step 1: Obtaining the Login Portal URL

1. Go to Cloud Organization > Identity Center as an Identity Center administrator.
2. In the left sidebar, click Identity Center Overview.
3. On the right side of the overview page, view or copy the user login URL.

Step 2: Logging In to the Identity Center User Portal

1. Click User Login URL as an Identity Center user to access the URL.

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

   > Note:
   >
   > SSO is supported for users, while user password login is not supported currently.

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

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

Step 3: Accessing Accounts

Logging In as a CAM User

After configuring CAM user synchronization in Identity Center, you can access account resources as a CAM user. For the configuration method, see Configuring CAM User Synchronization.
On the CAM User Login tab, click Log In in the Operation column of the target account. If you have access to multiple accounts, you can flexibly select the account you want to access on this page.

> Note:
>
> If the list is empty, you do not have access to any account.

FAQs
Operation FAQs

1. What Users Is Cloud Organization Suitable for?

Cloud Organization is suitable for group headquarters to manage multiple cloud platform root accounts within the enterprises.

2. Can I Change the Admin Account?

No. You cannot change the admin account.

3. How Do I Add a Cloud Platform Account to My Organization?

You can do this by inviting members or adding cloud platform accounts to your organization. For specific operations, see Adding an Organization Member.

4. Can a Cloud Platform Account Be a Member of Multiple Organizations?

No. A cloud platform root account can only be a member of one organization at a time.

5. How Do I Create a Department?

Cloud Organization supports up to five levels of departments. For specific operations, see Creating a Department.

1. Log in to Cloud Organization as an administrator.
2. In the left sidebar, select Department Management.
3. Navigate to the location where you want to create a unit in the hierarchy. You can directly create it under the root or in other units.
4. Click Add Department, and then provide a name for the department. This name should be unique in your organization.

   > Note
   >
   > You can rename the department later.

6. How Can I Move a Member's Cloud Platform Account in/out of a Department?

For specific operations, see Moving Members.
Perform the following steps to add a member account to a department:

1. In the Cloud Organization console, select the Department Management tab.
2. Select a cloud platform account, and then select Move in Members or Remove Member.
3. In the dialog box, select the department to which you want to move the cloud platform account.

7. Can a Cloud Platform Account Be a Member of Multiple Departments?

No. A cloud platform account can only be a member of one department.

8. How Many Levels of Departments Can an Organization Have?

You can nest up to five levels of departments. Your department hierarchy can have up to five levels of department nodes, including the root account and cloud platform accounts created in the lowest department.

API Documentation
Cam Identity Center(cic) version(2021-03-31)
API overview

API version

V3

Identity Center Management APIs

Interface name	Interface function
DescribeIdentityCenter	DescribeIdentityCenter
GetZoneStatistics	GetZoneStatistics
OpenIdentityCenter	OpenIdentityCenter
UpdateZone	UpdateZone

Identity Center Management SCIM Synchronization APIs

Interface name	Interface function
CreateSCIMCredential	CreateSCIMCredential
DeleteSCIMCredential	DeleteSCIMCredential
GetSCIMSynchronizationStatus	GetSCIMSynchronizationStatus
ListSCIMCredentials	ListSCIMCredentials
UpdateSCIMCredentialStatus	UpdateSCIMCredentialStatus
UpdateSCIMSynchronizationStatus	UpdateSCIMSynchronizationStatus

Identity Center Multi-Account Authorization Management APIs

Interface name	Interface function
CreateRoleAssignment	CreateRoleAssignment

Identity Center Permission Configuration Management APIs

Interface name	Interface function
CreateRoleConfiguration	CreateRoleConfiguration

Identity Center Single Sign-On Management APIs

Interface name	Interface function
AddExternalSAMLIdPCertificate	AddExternalSAMLIdPCertificate
ClearExternalSAMLIdentityProvider	ClearExternalSAMLIdentityProvider
GetExternalSAMLIdentityProvider	GetExternalSAMLIdentityProvider
GetZoneDetail	GetZoneDetail
GetZoneSAMLServiceProviderInfo	GetZoneSAMLServiceProviderInfo
ListExternalSAMLIdPCertificates	ListExternalSAMLIdPCertificates
RemoveExternalSAMLIdPCertificate	RemoveExternalSAMLIdPCertificate
SetExternalSAMLIdentityProvider	SetExternalSAMLIdentityProvider

Identity Center Sub-User Synchronization Management APIs

Interface name	Interface function

Interface name	Interface function
CreateUserSyncProvisioning	CreateUserSyncProvisioning
DeleteUserSyncProvisioning	DeleteUserSyncProvisioning
GetProvisioningTaskStatus	GetProvisioningTaskStatus
GetUserSyncProvisioning	GetUserSyncProvisioning
ListUserSyncProvisionings	ListUserSyncProvisionings
UpdateUserSyncProvisioning	UpdateUserSyncProvisioning

Identity Center User Group Management APIs

Interface name	Interface function
AddUserToGroup	AddUserToGroup
CreateGroup	CreateGroup
DeleteGroup	DeleteGroup
GetGroup	GetGroup
ListGroupMembers	ListGroupMembers
ListGroups	ListGroups
ListJoinedGroupsForUser	ListJoinedGroupsForUser
RemoveUserFromGroup	RemoveUserFromGroup
UpdateGroup	UpdateGroup

Identity Center User Management APIs

Interface name	Interface function
CreateUser	CreateUser
DeleteUser	DeleteUser
GetUser	GetUser

Interface name	Interface function
ListUsers	ListUsers
UpdateUser	UpdateUser
UpdateUserStatus	UpdateUserStatus

CallingMethod signaturev1

Converge Cloud authenticates each access request, i.e. each request needs to include authentication information (Signature) in the common parameters to verify the identity of the requester.
The Signature is generated by the security credentials which include SecretId and SecretKey. If you don't have the security credentials yet, go to the API Key page to apply for them; otherwise, you cannot invoke the API.

1. Applying for Security Credentials

Before using the API for the first time, go to the API Key page to apply for security credentials.
Security credentials consist of SecretId and SecretKey:

- SecretId is used to identify the API requester.
- SecretKey is used to encrypt the signature string and verify it on the server.
- You must keep your security credentials private and avoid disclosure.

You can apply for the security credentials through the following steps:

1. Log in to the Converge Cloud Console.
2. Go to the Cloud API Key page.
3. On the API Key Management page, click Create Key to create a SecretId/SecretKey pair.

Note: Each account can have up to two pairs of SecretId/SecretKey.

2. Generating a Signature

With the SecretId and SecretKey, a signature can be generated. The following describes how to generate a signature:

Assume that the SecretId and SecretKey are:

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

Note: This is just an example. For actual operations, please use your own SecretId and SecretKey.

Take the Cloud Virtual Machine's request to view the instance list (DescribeInstances) as an example. When

you invoke this API, the request parameters may be as follows:

Parameter name	Description	Parameter value
Action	Method name	DescribeInstances
SecretId	Key ID	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	Current timestamp	1465185768
Nonce	Random positive integer	11886
Region	Region where the instance is located	luzon
InstanceIds.0	ID of the instance to query	ins-09dx96dg
Offset	Offset	0
Limit	Allowed maximum output	20
Version	API version number	2017-03-12

2.1. Sorting Parameters

First, sort all the request parameters in an ascending lexicographical order (ASCII code) by their names. Notes: (1) Parameters are sorted by their names instead of their values; (2) The parameters are sorted based on ASCII code, not in an alphabetical order or by values. For example, InstanceIds.2 should be arranged after InstanceIds.12. You can complete the sorting process using a sorting function in a programming language, such as the ksort function in PHP. The parameters in the example are sorted as follows:

```
{
    'Action' : 'DescribeInstances',
    'InstanceIds.0' : 'ins-09dx96dg',
    'Limit' : 20,
    'Nonce' : 11886,
    'Offset' : 0,
    'Region' : 'luzon',
    'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
    'Timestamp' : 1465185768,
    'Version': '2017-03-12',
}
```

When developing in another programming language, you can sort these sample parameters and it will work as long as you obtain the same results.

2.2. Concatenating a Request String

This step generates a request string.
Format the request parameters sorted in the previous step into the form of "parameter name"="parameter value". For example, for the Action parameter, its parameter name is "Action" and its parameter value is "DescribeInstances", so it will become Action=DescribeInstances after formatted.
Note: The "parameter value" is the original value but not the value after URL encoding.

Then, concatenate the formatted parameters with "&". The resulting request string is as follows:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. Concatenating the Signature Original String

This step generates a signature original string.
The signature original string consists of the following parameters:

1. HTTP method: POST and GET modes are supported, and GET is used here for the request. Please note that the method name should be in all capital letters.
2. Request host: the domain name of the request to view the list of instances (DescribeInstances) is cvm.convergecloud.com. The actual request domain name varies by the module to which the API belongs. For more information, see the instructions of the specific API.
3. Request path: The request path in the current version of Cloud API is fixed to / .
4. Request string: the request string generated in the previous step.

The concatenation rule of the signature original string is: Request method + request host + request path + ? + request string

The concatenation result of the example is:

```
GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. Generating a Signature String

This step generates a signature string.
First, use the HMAC-SHA1 algorithm to sign thesignature original stringobtained in the previous step, and then encode the generated signature using Base64 to obtain the final signature.

The specific code is as follows with the PHP language being used as an example:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit
=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPL
E&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

The final signature is:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

When developing in another programming language, you can sign and verify the original in the example above and it works as long as you get the same results.

3. Encoding a Signature String

The generated signature string cannot be directly used as a request parameter and must be URL encoded.

For example, if the signature string generated in the previous step is EliP9YW3pW28FpsEdkXt/+WcGeI= , the final signature string request parameter (Signature) is EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d, which will be used to generate the final request URL.

**Note: If your request method is GET, or the request method is POST and the Content-Type is application/x-www-form-urlencoded, then all the request parameter values need to be URL encoded (except the parameter key and the symbol of =) when sending the request. Non-ASCII characters need to be encoded with UTF-8 before URL encoding. **

Note: The network libraries of some programming languages automatically URL encode all parameters, in which case there is no need to URL encode the signature string; otherwise, two rounds of URL encoding will cause the signature to fail.

Note: Other parameter values also need to be encoded using RFC 3986. Use %XY in percent-encoding for special characters such as Chinese characters, where "X" and "Y" are hexadecimal characters (0-9 and uppercase A-F), and using lowercase will cause an error.

4. Signature Failure

The following situational error codes for signature failure may occur. Please resolve the errors accordingly.

Error code	Error description
AuthFailure.SignatureExpire	The signature is expired

Error code	Error description
AuthFailure.SecretIdNotFound	The key does not exist
AuthFailure.SignatureFailure	Signature error
AuthFailure.TokenFailure	Token error
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type)

5. Signature Demo

When calling API 3.0, you are recommended to use the corresponding Converge Cloud SDK 3.0, Swhich encapsulates the signature process, enabling you to focus on only the specific APIs provided by the product when developing. See SDK Center for more information. Currently, the following programming languages are supported:

- Python
- Java
- PHP
- Go
- Node

To further explain the signing process, we will use a programming language to implement the process described above. The request domain name, API and parameter values in the sample are used here. This goal of this example is only to provide additional clarification for the signature process, please see the SDK for actual usage.

The final output URL might be: https://cvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

Note: The key in the example is fictitious, and the timestamp is not the current time of the system, so if this URL is opened in the browser or called using commands such as curl, an authentication error will be returned: Signature expired. In order to get a URL that can work properly, you need to replace the SecretId and SecretKey in the example with your real credentials and use the current time of the system as the Timestamp.

Note: In the example below, even if you use the same programming language, the order of the parameters in the URL may be different for each execution. However, the order does not matter, as long as all the parameters are included in the URL and the signature is calculated correctly.

Note: The following code is only applicable to API 3.0. It cannot be directly used in other signature processes. Even with an older API, signature calculation errors may occur due to the differences in details. Please refer to the corresponding documentation.

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class CloudAPIDemo {
    private final static String CHARSET = "UTF-8";

    public static String sign(String s, String key, String method) throws Exception {
        Mac mac = Mac.getInstance(method);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
        mac.init(secretKeySpec);
        byte[] hash = mac.doFinal(s.getBytes(CHARSET));
        return DatatypeConverter.printBase64Binary(hash);
    }

    public static String getStringToSign(TreeMap<String, Object> params) {
        StringBuilder s2s = new StringBuilder("GETcvm.convergecloud.com/?");
        // When signing, the parameters need to be sorted in lexicographical order. TreeMap is used here
to guarantee the correct order.
        for (String k : params.keySet()) {
            s2s.append(k).append("=").append(params.get(k).toString()).append("&");
        }
        return s2s.toString().substring(0, s2s.length() - 1);
    }

    public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException
{
        StringBuilder url = new StringBuilder("https://cvm.convergecloud.com/?");
        // There is no requirement for the order of the parameters in the actual request URL.
        for (String k : params.keySet()) {
            // The request string needs to be URL encoded. As the Key is all in English letters, only the valu
e is URL encoded here.
            url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).app
end("&");
        }
        return url.toString().substring(0, url.length() - 1);
```

```
    }

    public static void main(String[] args) throws Exception {
        TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap enables automati
c sorting
        // A random number should be used when actually calling, for example: params.put("Nonce", new
Random().nextInt(java.lang.Integer.MAX_VALUE));
        params.put("Nonce", 11886); // Common parameter
        // The current time of the system should be used when actually calling, for example:   params.put
("Timestamp", System.currentTimeMillis() / 1000);
        params.put("Timestamp", 1465185768); // Common parameter
        params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // Common parameter
        params.put("Action", "DescribeInstances"); // Common parameter
        params.put("Version", "2017-03-12"); // Common parameter
        params.put("Region", "luzon"); // Common parameter
        params.put("Limit", 20); // Business parameter
        params.put("Offset", 0); // Business parameter
        params.put("InstanceIds.0", "ins-09dx96dg"); // Business parameter
        params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE
", "HmacSHA1")); // Common parameter
        System.out.println(getUrl(params));
    }
}
```

Python

Note: If running in a Python 2 environment, the following requests dependency package must be installed first: pip install requests .

```
# -*- coding: utf8 -*-
import base64
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
    s = method + endpoint + "/?"
    query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
    return s + query_str

def sign_str(key, s, method):
```

```
    hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
    return base64.b64encode(hmac_str)

if __name__ == '__main__':
    endpoint = "cvm.convergecloud.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'luzon',
        'SecretId' : secret_id,
        'Timestamp' : 1465185768, # int(time.time())
        'Version': '2017-03-12'
    }
    s = get_string_to_sign("GET", endpoint, data)
    data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
    print(data["Signature"])
    # n actual invocation would occur here, which may incur fees after success
    # resp = requests.get("https://" + endpoint, params=data)
    # print(resp.url)
```

signaturev3

Converge Cloud The API will authenticate each access request, meaning that each request must include signature information (Signature) in the public request parameters to verify the requester's identity.
The signature information is generated by the security credentials, which include SecretId and SecretKey . If the user does not have security credentials, please apply for them on the Cloud API Key page, otherwise they cannot call the Cloud API interfaces.

1. Apply for security credentials.

Before using the Cloud API for the first time, please go to the Cloud API Key page to apply for a security credential.
Security credentials include SecretId and SecretKey:

- SecretId The security credentials are used to identify the identity of the API caller.
- SecretKey The secret key is used to encrypt and sign the string for server-side verification of the signature.
- Users must strictly protect their security credentials and avoid disclosure them.

The specific steps to apply for security credentials are as follows:

1. Log in to Converge Cloud Administration Center Console
2. Go to the console page for cloud API keys
3. On the Cloud API Key page, click New to create a pair of SecretId/SecretKey

Note: Developer accounts can have up to two pairs SecretId / SecretKey.

2. TC3-HMAC-SHA256 signature method

Note: For GET method, only Content-Type: application/x-www-form-urlencoded protocol format is supported. For POST method, Content-Type: application/json and Content-Type: multipart/form-data are currently supported. By default, all business interfaces are supported in json format. Only specific business interfaces are supported in multipart format. In this case, the interface cannot be called in json format. Refer to the specific business interface document description.

The following takes Cloud Virtual Machine querying Region-1 instance list as an example to introduce the signature calculation process step by step. We only use two parameters for the query instance list: Limit and Offset, called using the GET method.

Assume that the SecretId and SecretKey of the user are AKIDz 8krbsJ 5yKBZQpn 74WFkmLPx 3EXAMPLE and Gu 5t9xGARNpq 86cd 98joQYCN3EXAMPLE, respectively.

2.1. splice specification request string

Concatenate CanonicalRequest strings in the following format:

```
CanonicalRequest =
  HTTPRequestMethod + '\n' +
  CanonicalURI + '\n' +
  CanonicalQueryString + '\n' +
  CanonicalHeaders + '\n' +
  SignedHeaders + '\n' +
  HashedRequestPayload
```

- HTTPRequestMethod: HTTP request methods (GET, POST), GET in this example;
- CanonicalURI: URI parameter, API 3.0 fixed to forward slash (/);
- CanonicalQueryString: Query string in the URL that initiates the HTTP request. For POST requests, it is fixed as an empty string. For GET requests, it is the question mark (?) in the URL. The following string content, this example value is: Limit=10&Offset=0. Note: CanonicalQueryString needs to be URL encoded.
- CanonicalHeaders: The header information of participating signature, at least including host and content-type, can also be added with customized header to improve the uniqueness and security of its own request. Splicing rules: 1) head key and value are uniformly converted to lowercase, and the first and last spaces are removed, and spliced according to the format of key:value\n;2) multiple heads are spliced according to the dictionary sorting of head key (lowercase). In this example: content-type: application/x-www-form-urlencoded\nhost: cvm.convergecloud.com\n
- SignedHeaders: The header information involved in the signature indicates which headers participate in the signature of this request, and the header content contained in CanonicalHeaders is one-to-one corresponding. content-type and host are required headers. constructed as: 1) The head key is uniformly converted to lowercase; 2) Multiple header keys (lowercase) are concatenated according to dictionary sorting and separated by semicolons (;). In this case: content-type;host
- HashedRequestPayload: The hash value of the request body, calculated as Lowercase(HexEncode(Hash.SHA256(RequestPayload))), SHA256 hash the entire payload of the HTTP request body, then hexadecimal encoding, and finally converting the encoding string to lowercase letters. Note: For GET requests, RequestPayload is fixed as an empty string. For POST requests, RequestPayload is the payload of the HTTP request body.

According to the above rules, the resulting canonical request string in the example is as follows (for clarity, \nnewlines are replaced by a new line printed separately):

```
GET
```

```
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.convergecloud.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. Concatenate the string to be signed

Concatenate the string to be signed in the following format:

```
StringToSign =
  Algorithm + \n +
  RequestTimestamp + \n +
  CredentialScope + \n +
  HashedCanonicalRequest
```

- Algorithm: Signature algorithm, currently fixed as TC3-HMAC-SHA256;
- RequestTimestamp: Request timestamp, i.e. the X-TC-Timestamp value of the request header. The request in the example above is 1539084154;
- CredentialScope: Credential range in the format Date/service/tc3_request, containing date, requested service and termination string (tc3_request). **Date is the date of UTC standard time, the value needs to be consistent with UTC standard time converted by common parameter X-TC-Timestamp **;service is the product name, which must be consistent with the product domain name called, such as cvm. The above example request, the value is 2018-10-09/cvm/tc3_request;
- HashedCanonicalRequest: The hash value of the canonical request string obtained by concatenating the above steps is calculated by Lowercase(HexEncode(Hash.SHA256(CanonicalRequest))).

note:

> 1. Date must be calculated from timestamp X-TC-Timestamp and time zone UTC+0. Adding local time zone information to the system, such as East Zone 8, will cause calls to succeed during the day and night, but calls to fail in the early hours of the morning. Assuming the timestamp is 1551113065, the time in the East Eight District is 2019-02-26 00:44:25, but the calculated Date with UTC+0 should be 2019-02-25 instead of 2019-02-26.
> 2. Timestamp must be the current system time and ensure that the system time and standard time are synchronized. If the difference exceeds five minutes, it will fail. If it is not synchronized with the standard time for a long time, it may cause the request to fail after running for a period of time (return signature expiration error).

According to the above rules, the string to be signed in the example is as follows (for clarity,\nnewlines are

replaced by new lines printed):

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. calculate the signature

1. Compute the derived signature key, pseudocode as follows

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey: Original SecretKey;
- Date: That is, the Date field information in Credential, as shown in the example above, is 2018-10-09.;
- Service: That is, the Service field information in Credential, as shown in the example above, is cvm;

2. Calculate the signature, pseudocode as follows

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning: That is, the derivative signature key calculated above;
- StringToSign: That is, the character string to be signed calculated in step 2;

2.4. Splicing Authorization

Splice as follows Authorization:

```
Authorization =
    Algorithm + ' ' +
    'Credential=' + SecretId + '/' + CredentialScope + ', ' +
    'SignedHeaders=' + SignedHeaders + ', '
    'Signature=' + Signature
```

- Algorithm: Signature method, fixed as TC3-HMAC-SHA256;
- SecretId: SecretId in key pair;
- CredentialScope: See above, Scope of Voucher;
- SignedHeaders: See above, header information for participating signatures;
- Signature: signature value

According to the above rules, the values obtained in the example are:

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

The final complete invocation information is as follows:

```
https://cvm.convergecloud.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.convergecloud.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: luzon
```

3. signing failed

According to the actual situation, there are the following signature failure error codes, please handle according to the actual situation

error code	error description
AuthFailure.SignatureExpire	signature expiration
AuthFailure.SecretIdNotFound	key is not present
AuthFailure.SignatureFailure	signature error
AuthFailure.TokenFailure	token error
AuthFailure.InvalidSecretId	Illegal key (not cloud API key type)

4. Signature Demo

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
```

```
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class CloudAPITC3Demo {
    private final static String CHARSET = "UTF-8";
    private final static String ENDPOINT = "cvm.convergecloud.com";
    private final static String PATH = "/";
    private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
    private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
    private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencode
d";
    private final static String CT_JSON = "application/json";
    private final static String CT_FORM_DATA = "multipart/form-data";

    public static byte[] sign256(byte[] key, String msg) throws Exception {
        Mac mac = Mac.getInstance("HmacSHA256");
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
        mac.init(secretKeySpec);
        return mac.doFinal(msg.getBytes(CHARSET));
    }

    public static void main(String[] args) throws Exception {
        String service = "cvm";
        String host = "cvm.convergecloud.com";
        String region = "luzon";
        String action = "DescribeInstances";
        String version = "2017-03-12";
        String algorithm = "TC3-HMAC-SHA256";
        String timestamp = "1539084154";
        //String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
        SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
        // Pay attention to the time zone, otherwise it is easy to make mistakes.
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ************* Step 1: Assemble the specification request string *************
```

```
        String httpRequestMethod = "GET";
        String canonicalUri = "/";
        String canonicalQueryString = "Limit=10&Offset=0";
        String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host
+ "\n";
        String signedHeaders = "content-type;host";
        String hashedRequestPayload = DigestUtils.sha256Hex("");
        String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryStri
ng + "\n"
                + canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
        System.out.println(canonicalRequest);

        // ************* Step 2: Stitching the string to be signed *************
        String credentialScope = date + "/" + service + "/" + "tc3_request";
        String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
        String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCan
onicalRequest;
        System.out.println(stringToSign);

        // ************* Step 3: Calculate the signature *************
        byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
        byte[] secretService = sign256(secretDate, service);
        byte[] secretSigning = sign256(secretService, "tc3_request");
        String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLow
erCase();
        System.out.println(signature);

        // ************* Step 4: Splicing Authorization *************
        String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
                + "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
        System.out.println(authorization);

        TreeMap<String, String> headers = new TreeMap<String, String>();
        headers.put("Authorization", authorization);
        headers.put("Host", host);
        headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
        headers.put("X-TC-Action", action);
        headers.put("X-TC-Timestamp", timestamp);
        headers.put("X-TC-Version", version);
        headers.put("X-TC-Region", region);
    }
}
```

Python

```
# -*- coding: utf-8 -*-
```

```
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# key parameters
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.convergecloud.com"
endpoint = "https://" + host
region = "luzon"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ************* Step 1: Assemble the specification request string *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
payload = ""
if http_request_method == "POST":
    canonical_querystring = ""
    ct = "json"
    payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
                     canonical_uri + "\n" +
                     canonical_querystring + "\n" +
                     canonical_headers + "\n" +
                     signed_headers + "\n" +
                     hashed_request_payload)
print(canonical_request)

# ************* Step 2: Stitching the string to be signed *************
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
                  str(timestamp) + "\n" +
                  credential_scope + "\n" +
                  hashed_canonical_request)
print(string_to_sign)
```

```
# ************* Step 3: Calculate the signature *************
# Compute signature digest function
def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* Step 4: Splicing Authorization *************
authorization = (algorithm + " " +
                 "Credential=" + secret_id + "/" + credential_scope + ", " +
                 "SignedHeaders=" + signed_headers + ", " +
                 "Signature=" + signature)
print(authorization)

# Common parameters added to request header
headers = {
    "Authorization": authorization,
    "Host": host,
    "Content-Type": "application/%s" % ct,
    "X-TC-Action": action,
    "X-TC-Timestamp": str(timestamp),
    "X-TC-Version": version,
    "X-TC-Region": region,
}
```

request

1. Service Address

Region refers to the geographical area of a physical data center. Converge Cloud ensures complete isolation between different regions, providing maximum stability and fault tolerance. To reduce access latency and improve download speed, it is recommended to choose the region closest to your customers.

You can view the complete region list by using the API interface "DescribeRegions".

2. Communications Protocol

All the Converge Cloud APIs communicate via HTTPS, providing highly secure communication tunnels.

3. Request Methods

Supported HTTP request methods:

- POST (recommended)
- GET

PThe Content-Type types supported by POST requests:

- application/json (recommended). The TC3-HMAC-SHA256 signature algorithm must be used.
- application/x-www-form-urlencoded. The HmacSHA1 or HmacSHA256 signature algorithm must be used.
- multipart/form-data (only supported by certain APIs). You must use TC3-HMAC-SHA256 to calculate the signature.

The size of a GET request packet is up to 32 KB. The size of a POST request is up to 1 MB when the HmacSHA1 or HmacSHA256 signature algorithm is used, and up to 10 MB when TC3-HMAC-SHA256 is used.

4. Character Encoding

Only UTF-8 encoding is used.

result

Response for Successful Requests

For example, when calling CAM API (version: 2017-03-12) to view the status of instances (DescribeInstancesStatus), if the request has succeeded, you may see the response as shown below:

```
{
    "Response": {
        "TotalCount": 0,
        "InstanceStatusSet": [],
        "RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
    }
}
```

- The API will return Response, which contains RequestId, as long as it processes the request. It does not matter if the request is successful or not.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.
- Except for the fixed fields, all fields are action-specified. For the definitions of action-specified fields, see the corresponding API documentation. In this example, TotalCount and InstanceStatusSet are the fields specified by the API DescribeInstancesStatus. 0 TotalCount means that the requester owns 0 CVM instance so the InstanceStatusSet is empty.

Response for Failed Requests

If the request has failed, you may see the response as shown below:

```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```

- The presence of the Error field indicates that the request has failed. A response for a failed request will include Error, Code and Message fields.

- Code is the code of the error that helps you identify the cause and solution. There are two types of error codes so you may find the code in either common error codes or API-specified error codes.
- Message explains the cause of the error. Note that the returned messages are subject to service updates. The information the messages provide may not be up-to-date and should not be the only source of reference.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.

Common Error Codes

If there is an Error field in the response, it means that the API call failed. The Code field in Error indicates the error code. The following table lists the common error codes that all actions can return.

Error Code	Description
AuthFailure.InvalidSecretId	Invalid key (not a API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	The key does not exist.
AuthFailure.SignatureExpire	Signature expired.
AuthFailure.SignatureFailure	Signature error.
AuthFailure.TokenFailure	Token error.
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.

Error Code	Description
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	hHTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

PublicParameter

Common parameters are parameters used to identify users and interface authentication purposes. If not necessary, these parameters are not described in the separate interface document of each interface, but these parameters need to be carried in each request before the request can be normally initiated.

signature method v3

When using TC3-HMAC-SHA256 signature method, the common parameters need to be uniformly placed in the HTTP Header request header, as follows:

parameter name	type	required	described
X-TC-Action	String	Yes	The name of the operation interface. Refer to the description of the public parameter Action in the input parameters of the interface documentation for the value. For example, the value for the query instance list interface of the cloud server is DescribeInstances.
X-TC-Region	String	Yes	region parameters, Data used to identify which region you wish to operate on. The region value accepted by the interface refers to the description of the input parameter common parameter Region in the interface document. Note: Some interfaces do not need to pass this parameter, which is specifically stated in the interface documentation. In this case, even passing this parameter will not take effect.
X-TC-Timestamp	Integer	Yes	The current UNIX timestamp, which records the time when the API request was initiated. for example 1529223702. Note: If the time difference from the server exceeds 5 minutes, it will cause a signature expiration error.
X-TC-Version	String	Yes	Version of API for operation. Refer to the description of the public parameter Version in the interface document for the value. For example, the version of the cloud server. 2017-03-12.
Authorization	String	Yes	HTTP The standard authentication header field is "Authorization". For example: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 Here, - TC3-HMAC-SHA256: Signature method, currently fixed as this value, - Credential: Credential: Signature credential; AKIDEXAMPLE is the SecretId; Date is a date in UTC time, and this value must match the value of X-TC-Timestamp (a common parameter) in UTC time format; service is the name of the product/service, and is generally a domain name prefix. For example,cvm; - SignedHeaders: The headers that contains the authentication information; content-type and host are the required headers; - Signature: Signature digest.
X-TC-Token	String	No	The token used for temporary certificates needs to be used in conjunction with a temporary key. Temporary keys and tokens need to be obtained by calling the access management service interface. Long-term keys do not require tokens.

signature method v1

When using HmacSHA1 and HmacSHA256 signature methods, common parameters need to be placed uniformly in the request string, as follows

parameter name	type	required	described
Action	String	Yes	The name of the interface to be operated. The value refers to the explanation of the public parameter Action in the interface documentation. For example, for the cloud server's query instance list interface, the value is DescribeInstances .
Region	String	Yes	The region parameter is used to identify which region's data you want to operate on. The region value accepted by the interface is specified in the input parameter of the public parameter Region in the interface documentation. Note: Some interfaces do not require this parameter to be passed, which will be specifically mentioned in the interface documentation. Even if this parameter is passed, it will not take effect in this case.
Timestamp	Integer	Yes	The current UNIX timestamp, which can record the time when the API request is initiated. For example, 1529223702. If the difference between the current time is too large, it will cause a signature expiration error.
Nonce	Integer	Yes	A random positive integer combined with Timestamp is used to prevent replay attacks.
SecretId	String	Yes	The SecretId is an identifier applied for the cloud API key to identify the user's identity. A SecretId corresponds to a unique SecretKey , and the SecretKey is used to generate the request signature Signature .
Signature	String	Yes	Request signature is used to verify the legitimacy of this request. Users need to calculate it based on the actual input parameters. The specific calculation method can be found in the interface authentication documentation.
Version	String	Yes	The version of the API being operated on. The value refers to the description of the public parameter Version in the interface documentation. For example, the version of the cloud server. 2017-03-12.
SignatureMethod	String	No	Signature method, currently supports HmacSHA256 and HmacSHA1. HmacSHA256 algorithm is used to verify signatures only if this parameter is specified as HmacSHA 256, otherwise HmacSHA1 is used to verify signatures.
Token	String	No	Token used for temporary certificate needs to be used together with temporary key. The temporary key and Token need to be obtained from the Access Management service invocation interface. Long-term keys do not require tokens.

zone list

A region (Region) refers to the geographical area of a physical data center. Converge Cloud Translation: To deliver verification that completely isolates different regions, ensuring maximum stability and fault tolerance between regions. In order to reduce access latency and improve download speed, it is recommended that you choose the region closest to your customers.

You can view the complete region list by using the API interface Query Region List.

Identity Center Management APIs
DescribeIdentityCenter

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to obtain TCO Identity Center service information.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIdentityCenter
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
ZoneId	String	Space ID, which starts with the z- prefix, followed by 12 random digits/lowercase letters. Example: z-2d8shd8***
ZoneName	String	Space name, which should be globally unique and contain 2– 64 characters including lowercase letters, digits, and hyphens (-). It can neither start or end with a hyphen (-) nor contain two consecutive hyphens (-). Example: zone_name
ServiceStatus	String	Service activation status. Disabled: not activated; Enabled: activated. Example: Enabled
ScimSyncStatus	String	SCIM synchronization status. Enabled: enabled. Disabled: disabled. Example: Enabled
CreateTime	String	Creation Time Example: 2025-01-03 12:12:23
UpdateTime	String	Update time Example: 2025-01-03 12:12:23
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.DBOperationError	
FailedOperation.IdentityCenterNotOpen	

GetZoneStatistics

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to query space statistics.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: GetZoneStatistics
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Zone ID Example: z-2d8shd8***

3. Output Parameters

Parameter name	Type	Description
ZoneStatistics	ZoneStatistics	Space statistics. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	

OpenIdentityCenter

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to activate Identity Center service (CIC).

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: OpenIdentityCenter
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneName	Yes	Yes	String	Space name, which should be globally unique and contain 2– 64 characters including lowercase letters, digits, and hyphens (-). It can neither start or end with a hyphen (-) nor contain two consecutive hyphens (-). Example: zone_name

3. Output Parameters

Parameter name	Type	Description
ZoneId	String	Space ID, which starts with the z- prefix, followed by 12 random digits/lowercase letters. Example: z-2d8shd8***
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.ServiceRoleNotExist	
FailedOperation.DBOperationError	
FailedOperation.IdentityCenterAlreadyOpen	
FailedOperation.IdentityCenterNotAuth	
FailedOperation.IdentityCenterNotEnterpriseAuth	
FailedOperation.IdentityCenterOrganizationNotOpen	
FailedOperation.IdentityCenterNotOrganizationManager	
InvalidParameterValue.IdentityCenterZoneNameAlreadyExist	

UpdateZone

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to update the user's space name.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateZone
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID, which starts with the z- prefix, followed by 12 random digits/lowercase letters. Example: z-2d8shd8***
NewZoneName	Yes	Yes	String	Space name, which should be globally unique and contain 2– 64 characters including lowercase letters, digits, and hyphens (-). It can neither start or end with a hyphen (-) nor contain two consecutive hyphens (-). Example: zone_name

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.ZoneNameFormatError	
FailedOperation.ZoneIdNotExist	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.DBOperationError	

Identity Center Management SCIM Synchronization APIs CreateSCIMCredential

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to create a SCIM key.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateSCIMCredential
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID, which starts with the z- prefix, followed by 12 random digits/ lowercase letters. Example: z-2d8shd8***

3. Output Parameters

Parameter name	Type	Description
CreateTime	String	Creation time of a SCIM key. Example: 2025-01-03 12:12:23
ExpireTime	String	Expiration time of a SCIM key. Example: 2025-01-03 12:12:23
CredentialStatus	String	SCIM key status. Enabled: enabled. Disabled: disabled. Example: Enabled
CredentialSecret	String	SCIM key. Example: sJf[mc5kPJ8saXeYDgyw****
ZoneId	String	Space ID, which starts with the z- prefix, followed by 12 random digits/ lowercase letters. Example: z-2d8shd8***
CredentialId	String	SCIM key ID, which starts with the scimcred- prefix, followed by 12 random digits/lowercase letters. Example: scimcred-lkj****
CredentialType	String	SCIM key type. Example: BearerToken
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.DBOperationError	
LimitExceeded.ScimCredentialLimitExceeded	
FailedOperation.ScimCredentialGenerateError	

DeleteSCIMCredential

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to delete a SCIM Key.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteSCIMCredential
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID, which starts with the z- prefix, followed by 12 random digits/ lowercase letters. Example: z-2d8shd8***
CredentialId	Yes	Yes	String	SCIM key ID, which starts with the scimcred- prefix, followed by 12 random digits/ lowercase letters. Example: scimcred-lkj****

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.DBOperationError	
FailedOperation.IdentityCenterNotOpen	
InvalidParameter.ScimCredentialNotFound	
FailedOperation.ZoneIdNotExist	

GetSCIMSynchronizationStatus

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to query SCIM synchronization status.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: GetSCIMSynchronizationStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID, which starts with the z- prefix, followed by 12 random digits/lowercase letters. Example: z-2d8shd8***

3. Output Parameters

Parameter name	Type	Description
SCIMSynchronizationStatus	String	SCIM synchronization status. Enabled: enabled. Disabled: disabled. Example: Enabled
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.ZoneIdNotExist	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.DBOperationError	

ListSCIMCredentials

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to query the user SCIM key list.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ListSCIMCredentials
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID, which starts with the z- prefix, followed by 12 random digits/ lowercase letters. Example: z-2d8shd8***
CredentialId	No	Yes	String	SCIM key ID. Example: scimcred-lkj****

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
TotalCounts	Int64	Number of SCIM keys. Example: 1
SCIMCredentials	Array of SCIMCredential	SCIM key information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.DBOperationError	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	

UpdateSCIMCredentialStatus

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to enable or disable a SCIM key.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateSCIMCredentialStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID, which starts with the z- prefix, followed by 12 random digits/lowercase letters. Example: z-2d8shd8***
CredentialId	Yes	Yes	String	SCIM key ID, which starts with the scimcred- prefix, followed by 12 random digits/lowercase letters. Example: scimcred-lkj****
NewStatus	Yes	Yes	String	SCIM key status. Enabled: enabled. Disabled: disabled. Example: Enabled

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.ZoneIdNotExist	
InvalidParameter.UserScimCredentialStatusError	
InvalidParameter.ScimCredentialNotFound	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.DBOperationError	

UpdateSCIMSynchronizationStatus

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to enable or disable user SCIM synchronization.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateSCIMSynchronizationStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID, which starts with the z- prefix, followed by 12 random digits/lowercase letters. Example: z-2d8shd8***
SCIMSynchronizationStatus	Yes	Yes	String	SCIM synchronization status. Enabled: enabled. Disabled: disabled. Example: Enabled

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.DBOperationError	

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
InvalidParameter.ScimSyncStatusError	

Identity Center Multi-Account Authorization Management APIs CreateRoleAssignment

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to grant authorizations on member accounts.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateRoleAssignment
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
RoleAssignmentInfo	No	Yes	Array of RoleAssignmentInfo	Authorized member account information, up to 50 entries. Example:View

3. Output Parameters

Parameter name	Type	Description
Tasks	Array of TaskInfo	Task details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.UserNotExist	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
InvalidParameter.GroupNotExist	
InvalidParameter.RoleConfigurationNotExist	
FailedOperation.OrganizationMemberNotExist	
FailedOperation.RoleConfigurationAuthorizationAlreadyExist	
FailedOperation.RoleConfigurationAuthorizationOverLimit	
LimitExceeded.CreateRoleAssignmentLimitExceeded	

Identity Center Permission Configuration Management APIs
CreateRoleConfiguration

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

Create permission configuration

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateRoleConfiguration
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
RoleConfigurationName	Yes	Yes	String	Permission configuration name, which contains up to 128 characters, including English letters, digits, and hyphens (-). Example: conf1
Description	No	Yes	String	Permission configuration description, which contains up to 1024 characters. Example: description
SessionDuration	No	Yes	Int64	Session duration, in seconds. It is the maximum time a CIC user can maintain a session while using permission configurations to access a target account in TCO. Value range: 900 to 43200 (15 minutes to 12 hours). Default: 3600 (1 hour). Example: 900
RelayState	No	Yes	String	The initial access page URL visited by the CIC users when they uses permission configuration to access a target account in TCO. This page must be a cloud console page. It is empty by default, which means navigating to the cloud console homepage. Example: https://XXX

3. Output Parameters

Parameter name	Type	Description
RoleConfigurationInfo	RoleConfiguration	Access configuration details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.DBOperationError	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
InvalidParameter.ConfigurationNameAlreadyExists	
InvalidParameter.ConfigurationNameFormatError	
FailedOperation.ConfigurationOverUpperLimit	

Identity Center Single Sign-On Management APIs AddExternalSAMLIdPCertificate

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to add SAML signing certificates.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AddExternalSAMLIdPCertificate
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
X509Certificate	Yes	Yes	String	X509 certificate in PEM format, provided by the SAML identity provider. Example: MIIBtjCCAVugAwIBAgI*****
ZoneId	Yes	Yes	String	Space ID. Example: z-necd***

3. Output Parameters

Parameter name	Type	Description
CertificateId	String	SAML signing certificate ID. Example: idp-c-2jd8923je29****
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.X509CertificateFormatError	
FailedOperation.X509CertificateAlreadyExist	
FailedOperation.X509CertificateParsingFailed	
FailedOperation.DBOperationError	
InternalError	

ClearExternalSAMLIdentityProvider

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to clear the SAML identity provider configuration information.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ClearExternalSAMLIdentityProvider
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	
FailedOperation.DBOperationError	
ResourceNotFound.SAMLIdentityProviderNotFound	
FailedOperation.SSoStatusEnableNotClearIdentityProvider	

GetExternalSAMLIdentityProvider

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to query the SAML identity provider configuration information.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: GetExternalSAMLIdentityProvider
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***

3. Output Parameters

Parameter name	Type	Description
SAMLIdentityProviderConfiguration	SAMLIdentityProviderConfiguration	SAML identity provider configuration information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	

Error Code	Description
FailedOperation.DBOperationError	
ResourceNotFound.SAMLIdentityProviderNotFound	

GetZoneDetail

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to obtain the space information by space name.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-25 16:08:59.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: GetZoneDetail
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneName	Yes	Yes	String	Space name, which should be globally unique and contain 2– 64 characters including lowercase letters, digits, and hyphens (-). It can neither start or end with a hyphen (-) nor contain two consecutive hyphens (-). Example: zone_name

3. Output Parameters

Parameter name	Type	Description
ServiceStatus	String	Service activation status. Disabled: not activated; Enabled: activated. Example: Enabled
SSOStatus	String	SSO login enabling status. Valid values: Disabled and Enabled. Example: Enabled
IdpLoginUrl	String	IdP login URL when SSO login is enabled. Example: ttp://www.okta.com/exke***
IdpEntityID	String	idp entity ID. Example: http://www.okta.com/exk***
SAMLRequest	String	Authentication request sent by the SP to the IdP. Example: PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTg***
ZoneId	String	Space ID, which starts with the z- prefix, followed by 12 random digits/lowercase letters. Example: z-2d8shd8***
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.DBOperationError	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.IdentityProviderNotConfigured	

GetZoneSAMLServiceProviderInfo

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to query the SAML service provider configuration information.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: GetZoneSAMLServiceProviderInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***

3. Output Parameters

Parameter name	Type	Description
SAMLServiceProvider	SAMLServiceProvider	SAML service provider configuration information. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	
FailedOperation.DBOperationError	
ResourceNotFound.SAMLServiceProviderNotFound	
FailedOperation.SAMLMetadataDocumentGetFailed	

ListExternalSAMLIdPCertificates

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to query the SAML signing certificate list.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ListExternalSAMLIdPCertificates
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***

3. Output Parameters

Parameter name	Type	Description
TotalCounts	Int64	Total number of data entries that meet the request parameter conditions. Example: 1
SAMLIdPCertificates	Array of SAMLIdPCertificate	SAML signing certificate list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	
FailedOperation.DBOperationError	

RemoveExternalSAMLIdPCertificate

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to remove SAML signing certificates.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RemoveExternalSAMLIdPCertificate
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
CertificateId	Yes	Yes	String	X509 certificate in PEM format, provided by the SAML identity provider. Example: dp-c-2jd8923je29****
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	
FailedOperation.DBOperationError	
ResourceNotFound.X509CertificateNotFound	

SetExternalSAMLIdentityProvider

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to configure the SAML identity provider information.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: SetExternalSAMLIdentityProvider
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
EntityId	No	Yes	String	IdP identifier. Example: http://www.okta.com/2jd***
LoginUrl	No	Yes	String	IdP login URL. Example: https://dev***.okta.com
X509Certificate	No	Yes	String	X509 certificate in PEM format. If this parameter is specified, all existing certificates will be replaced. Example: MIIBtjCCAVugAwIBAgIT***
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
EncodedMetadataDocument	No	Yes	String	IdP metadata document (Base64 encoded). Provided by an IdP that supports the SAML 2.0 protocol. Example: PD94bWwgdmVyc2lvbj0iM***
SSOStatus	No	Yes	String	SSO enabling status. Valid values: Enabled, Disabled (default). Example: Enabled

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.X509CertificateFormatError	
FailedOperation.UploadMetadataFailed	
InvalidParameterValue.SSoStatusInvalid	
FailedOperation.SAMLServiceProviderCreateFailed	
FailedOperation.XMLDataUnmarshalFailed	
FailedOperation.DecodeMetadataDocumentFailed	

Error Code	Description
FailedOperation.X509CertificateParsingFailed	
FailedOperation.MetadataCosParsingFailed	
FailedOperation.DBOperationError	
InternalError	

Identity Center Sub-User Synchronization Management APIs CreateUserSyncProvisioning

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to create sub-user synchronization tasks.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateUserSyncProvisioning
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
UserSyncProvisionings	Yes	Yes	Array of UserSyncProvisioning	CAM user synchronization information. Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
Tasks	Array of UserProvisioningsTask	Task details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.UserNotExist	
InvalidParameter.GroupNotExist	
FailedOperation.UserProvisioningAlreadyExists	
FailedOperation.OrganizationMemberNotExist	
FailedOperation.UserProvisioningOverLimit	
LimitExceeded.CreateUserSyncProvisioningLimitExceeded	

DeleteUserSyncProvisioning

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to delete sub-user synchronization tasks.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteUserSyncProvisioning
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
UserProvisioningId	Yes	Yes	String	User synchronization ID. Example: up-sjisnw8ois

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
Tasks	UserProvisioningsTask	Task details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
ResourceNotFound.UserProvisioningNotFound	
FailedOperation.UserProvisioningFailed	

GetProvisioningTaskStatus

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to query the status of async tasks of user synchronization.

Default interface request rate limit: 220 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: GetProvisioningTaskStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
TaskId	Yes	Yes	String	Task ID. Example: t-x8jd983n****

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
TaskStatus	TaskStatus	Task status information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
ResourceNotFound.UserProvisioningTaskNotFound	

GetUserSyncProvisioning

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to query the CAM user synchronization.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: GetUserSyncProvisioning
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
UserProvisioningId	Yes	Yes	String	ID of the CAM user synchronization. Example: up-sjisnw8ois

3. Output Parameters

Parameter name	Type	Description
UserProvisioning	UserProvisioning	CAM user synchronization information.

Parameter name	Type	Description
		Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
ResourceNotFound.UserProvisioningNotFound	

ListUserSyncProvisionings

1. Interface Description

Interface request domain name: cic.api.convergecloud.com.

This API is used to query the CAM user synchronization list.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ListUserSyncProvisionings
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
TargetUin	No	Yes	Int64	UIN of the target account of the TCO. Example: 111111111111
TargetType	No	Yes	String	Type of the synchronized target account of the TCO. ManagerUin: admin account; MemberUin: member account. Example: MemberUin
Filter	No	Yes	String	Detection condition. Example: user1
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
PrincipalId	No	Yes	String	User synchronization ID. Valid values: When PrincipalType is Group, it is a user group ID (g-). When PrincipalType is User, it is a user ID (u-).
NextToken	No	Yes	String	Token for querying the next page of returned results. During use of the API for the first time, NextToken is not needed. When you call the API for the first time, if the total number of returned data entries exceeds the MaxResults limit, the data is truncated and only MaxResults data entries are returned. Meanwhile, the return parameter IsTruncated is true and a NextToken is returned. You can use the NextToken returned last time to continue calling the API with other request parameters unchange
MaxResults	No	Yes	Int64	Maximum number of data entries per page. Value range: 1–100. Default value: 10. Example: 1
PrincipalType	No	Yes	String	Type of the object for CAM user synchronization. Valid values: User: an Identity Center user. Group: an Identity Center user group. Example: User

3. Output Parameters

Parameter name	Type	Description
MaxResults	Int64	Maximum number of data entries per page. Example: 1
IsTruncated	Bool	Whether the returned result is truncated. Valid values: true: truncated; false: not truncated. Example: true
UserProvisionings	Array of UserProvisioning	User list of the CAM synchronization. Example:View
NextToken	String	Token for querying the next page of returned results. Note: This parameter is displayed only when IsTruncated is true. Example: sjdhdhw
TotalCounts	Int64	Total number of data entries that meet the request parameter conditions. Example: 1
RequestId	String	Unique request id. Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
InvalidParameter.NextTokenInvalid	

UpdateUserSyncProvisioning

1. Interface Description

Interface request domain name: cic.api.1.convergecloud.com.

This API is used to create sub-user synchronization tasks.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateUserSyncProvisioning
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
NewDescription	No	Yes	String	User synchronization description. Example: description
NewDuplicationStrateful	No	Yes	String	Conflict policy. It indicates the handling policy for existence of a user with the same username when CIC users are synchronized to CAM. Valid values: KeepBoth: Keep both, that is, add the _cic suffix to the CIC user's username and then try to create a CAM user with the username when CIC users are synchronized to CAM and a user with the same username already exists in CAM; TakeOver: Replace, that is, directly replace the existing CAM user with the synchronized CIC user when CIC u Example: KeepBoth
NewDeletionStrategy	No	Yes	String	Deletion policy. It indicates the handling policy for CAM users already synchronized when the CAM user synchronization is deleted. Valid values: Delete: Delete the CAM users already synchronized from CIC to CAM when the CAM user synchronization is deleted; Keep: Keep the CAM users already synchronized from CIC to CAM when the CAM user synchronization is deleted. . Example: Delete
ZoneId	Yes	Yes	String	Space ID. Example: z-2s8xhs8***
UserProvisioningId	Yes	Yes	String	User synchronization ID. Example: up-ajsnwx8zra

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
ResourceNotFound.UserProvisioningNotFound	

Identity Center User Group Management APIs
AddUserToGroup

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to add users to a user group.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AddUserToGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
GroupId	Yes	Yes	String	User group ID. Example: g-2xdb82n8***
UserId	Yes	Yes	String	User ID. Example: u-28sh72be

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.GroupTypeUserTypeNotMatch	
FailedOperation.ManualGroupNotUpdate	
LimitExceeded.AddUserToGroupLimitExceeded	
FailedOperation.UserAddGroupCountOverUpperLimit	
FailedOperation.GroupUserCountOverUpperLimit	
InvalidParameter.GroupUserAlreadyExists	
FailedOperation.SynchronizedGroupNotAddUser	
FailedOperation.SynchronizedGroupNotUpdate	
InvalidParameter.GroupNotExist	
FailedOperation.ZoneIdNotExist	
FailedOperation.IdentityCenterNotOpen	
ResourceNotFound.UserNotExist	

CreateGroup

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

Create User Group

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
GroupName	Yes	Yes	String	User group name, which contains up to 128 characters, including English letters, digits, and special characters (-). Example: group_name
Description	No	Yes	String	User group description, which contains up to 1024 characters. Example: description
GroupType	No	Yes	String	User group type. Manual: manually created, Synchronized: imported from external sources. Example: Manual

3. Output Parameters

Parameter name	Type	Description
GroupInfo	GroupInfo	User group information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
InvalidParameter.GroupNameFormatError	
InvalidParameter.GroupNameAlreadyExists	
FailedOperation.GroupOverUpperLimit	

DeleteGroup

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

Delete a user group

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
GroupId	Yes	Yes	String	User group ID. Example: g-2e92j3***

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.ManualGroupNotDelete	
FailedOperation.RoleConfigurationAuthorizationExist	
FailedOperation.UserProvisioningExists	
FailedOperation.DeleteGroupNotAllowExistUser	
FailedOperation.SynchronizedGroupNotDelete	
InvalidParameter.GroupNotExist	
FailedOperation.ZoneIdNotExist	
FailedOperation.IdentityCenterNotOpen	

GetGroup

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to query the user group information.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: GetGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
GroupId	Yes	Yes	String	User group ID. Example: g-sd8sh8sdno***

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
GroupInfo	GroupInfo	User group info Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
InvalidParameter.GroupNotExist	

ListGroupMembers

1. Interface Description

Interface request domain name: cic.api.convergecloud.com.

This API is used to query the user list of the user group.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ListGroupMembers
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
UserType	No	Yes	String	User type. Manual: manually created; Synchronized: externally imported. Example: Manual
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
GroupId	Yes	Yes	String	User group ID. Example: g-sd8shbdsns***
NextToken	No	Yes	String	Token for querying the next page of returned results. During use of the API for the first time, NextToken is not needed. When you call the API for the first time, if the total number of returned data entries exceeds the MaxResults limit, the data is truncated and only MaxResults data entries are returned. Meanwhile, the return parameter IsTruncated is true and a NextToken is returned. You can use the NextToken returned last time to continue calling the API with other request parameters unchanged. Example: sjdhdhw
MaxResults	No	Yes	Int64	Maximum number of data entries per page. Value range: 1–100. Default value: 10. Example: 1

3. Output Parameters

Parameter name	Type	Description
NextToken	String	Token for querying the next page of returned results. Note: This parameter is displayed only when IsTruncated is true. Example: sjdhdhw
TotalCounts	Int64	Total number of data entries that meet the request parameter conditions. Example: 1
MaxResults	Int64	Maximum number of data entries per page. Example: 1
IsTruncated	Bool	Whether the returned result is truncated. Valid values: true: truncated; false: not truncated. Example: true
GroupMembers	Array of GroupMembers	The user list of a user group. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
InvalidParameter.GroupNotExist	

ListGroups

1. Interface Description

Interface request domain name: cic.api.convergecloud.com.

Query user group list

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ListGroups
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
NextToken	No	Yes	String	Token for querying the next page of returned results. During use of the API for the first time, NextToken is not needed. When you call the API for the first time, if the total number of returned data entries exceeds the MaxResults limit, the data is truncated and only MaxResults data entries are returned. Meanwhile, the return parameter IsTruncated is true and a NextToken is returned. You can use the NextToken returned last time to continue calling the API with other request parameters unchanged. Example: sjdhdhw
Filter	No	Yes	String	Filter criterion. Format: , case-insensitive. Currently, supports only GroupName, and supports only eq (Equals) and vw (Start With). For example, Filter = "GroupName sw test" indicates querying all user groups with names starting with test; Filter = "GroupName eq testgroup" indicates querying the user group with the name testgroup. Example: user1
GroupType	No	Yes	String	User group type. Manual: manually created; Synchronized: externally imported. Example: Manual
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shs8f***
FilterUsers	No	Yes	Array of String	Filtered user. IsSelected=1 will be returned for the user group associated with this user. Example: user1
SortField	No	Yes	String	Sorting field, which currently only supports CreateTime. The default is the CreateTime field. Example: CreateTime
SortType	No	Yes	String	Sorting order. Desc: descending order; Asc: ascending order. It should be set together with SortField. Example: Desc
Offset	No	Yes	Int64	Pagination offset. Do not use it together with NextToken, prioritizing using NextToken. Example: 0
MaxResults	No	Yes	Int64	Maximum number of data entries per page. Value range: 1–100. Default value: 10. Example: 1

3. Output Parameters

Parameter name	Type	Description
MaxResults	Int64	Maximum number of data entries per page. Example: 1
TotalCounts	Int64	Total number of data entries that meet the request parameter conditions. Example: 1
IsTruncated	Bool	Whether the returned result is truncated. Valid values: true: truncated; false: not truncated. Example: true
NextToken	String	Token for querying the next page of returned results. Note: This parameter is displayed only when IsTruncated is true. Example: sjdhdhw
Groups	Array of GroupInfo	User group list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter.ParamError	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
InvalidParameter.NextTokenInvalid	

ListJoinedGroupsForUser

1. Interface Description

Interface request domain name: cic.api.converge.com.

This API is used to query the user group joined by users.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ListJoinedGroupsForUser
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MaxResults	No	Yes	Int64	Maximum number of data entries per page. Value range: 1–100. Default value: 10. Example: 1
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
UserId	Yes	Yes	String	User ID Example: u-34nesn3u
NextToken	No	Yes	String	Token for querying the next page of returned results. During use of the API for the first time, NextToken is not needed. When you call the API for the first time, if the total number of returned data entries exceeds the MaxResults limit, the data is truncated and only MaxResults data entries are returned. Meanwhile, the return parameter IsTruncated is true and a NextToken is returned. You can use the NextToken returned last time to continue calling the API with other request parameters unchanged. Example: sjdhdhw

3. Output Parameters

Parameter name	Type	Description
IsTruncated	Bool	Whether the returned result is truncated. Valid values: true: truncated; false: not truncated. Example: true
JoinedGroups	Array of JoinedGroups	List of user groups joined by the user. Example:false
NextToken	String	Token for querying the next page of returned results. Note: This parameter is displayed only when IsTruncated is true. Example: sjdhdhw
TotalCounts	Int64	Total number of data entries that meet the request parameter conditions. Example: 1
MaxResults	Int64	Maximum number of data entries per page. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.UserNotExist	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	

RemoveUserFromGroup

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to remove users from a user group.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RemoveUserFromGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
GroupId	Yes	Yes	String	User group ID. Example: g-sd8sh8sdno***
UserId	Yes	Yes	String	User ID. Example: u-34nesn3u

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.ManualGroupNotUpdate	
LimitExceeded.RemoveUserFromGroupLimitExceeded	
InvalidParameter.GroupUserNotExist	
FailedOperation.SynchronizedGroupNotRemoveUser	
FailedOperation.SynchronizedGroupNotUpdate	
InvalidParameter.GroupNotExist	
FailedOperation.ZoneIdNotExist	
FailedOperation.IdentityCenterNotOpen	

UpdateGroup

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to modify user group information.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
GroupId	Yes	Yes	String	User group ID. Example: g-sd8sh8sdno***
NewGroupName	No	Yes	String	New user group name. Example: group_name
NewDescription	No	Yes	String	New user group description. Example: description
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***

3. Output Parameters

Parameter name	Type	Description
GroupInfo	GroupInfo	User group information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.ManualGroupNotUpdate	
FailedOperation.SynchronizedGroupNotUpdate	
InvalidParameter.GroupNotExist	
InvalidParameter.GroupNameAlreadyExists	
FailedOperation.ZoneIdNotExist	
FailedOperation.IdentityCenterNotOpen	

Identity Center User Management APIs
CreateUser

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

Create User

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateUser
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
FirstName	No	Yes	String	Last name of the user, which contains up to 64 characters. Example: Alice
Description	No	Yes	String	User description, which contains up to 1024 characters. Example: description
UserStatus	No	Yes	String	User status. Valid values: Enabled (default), Disabled. Example: Enabled
UserType	No	Yes	String	User type. Manual: manually created, Synchronized: imported from external sources. Example: Manual
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
LastName	No	Yes	String	First name of the user, which contains up to 64 characters. Example: Alice
DisplayName	No	Yes	String	Display name of the user, which contains up to 256 characters. Example: Alice
Email	No	Yes	String	Email address of the user, which should be unique within the directory and contains up to 128 characters. Example: Alice@example.com
UserName	Yes	Yes	String	User name, which must be unique within the space and cannot be modified. It contains up to 64 characters, including digits, English letters, and special characters such as plus signs (+), equal signs (=), commas (,), periods (.), at signs (@), hyphens (-), and underscores (_). Example: Alice

3. Output Parameters

Parameter name	Type	Description
UserInfo	UserInfo	User Details Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
InvalidParameter.UsernameFormatError	
InvalidParameter.UsernameAlreadyExists	
InvalidParameter.EmailAlreadyExists	
FailedOperation.UserOverUpperLimit	
LimitExceeded.CreateUserLimitExceeded	

DeleteUser

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

Delete user

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteUser
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
UserId	Yes	Yes	String	User ID. Example: u-34nesn3u

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.ManualUserNotDelete	
FailedOperation.RoleConfigurationAuthorizationExist	
FailedOperation.UserProvisioningExists	
InvalidParameter.UserAlreadyExistsGroup	
FailedOperation.SynchronizedUserNotDelete	
FailedOperation.ZoneIdNotExist	
FailedOperation.IdentityCenterNotOpen	
ResourceNotFound.UserNotExist	

GetUser

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to query user information.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: GetUser
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
UserId	Yes	Yes	String	User ID. Example: u-34nesn3u

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
UserInfo	UserInfo	User information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.UserNotExist	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	

ListUsers

1. Interface Description

Interface request domain name: cic.api.converge.com.

Query user list

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ListUsers
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
Filter	No	Yes	String	Filter criterion, which currently only supports username, email address, userId, and description. Example: user1
NextToken	No	Yes	String	Token for querying the next page of returned results. During use of the API for the first time, NextToken is not needed. When you call the API for the first time, if the total number of returned data entries exceeds the MaxResults limit, the data is truncated and only MaxResults data entries are returned. Meanwhile, the return parameter IsTruncated is true and a NextToken is returned. You can use the NextToken returned last time to continue calling the API with other request parameters unchange Example: sjdhdhw
FilterGroups	No	Yes	Array of String	Filtered user group. IsSelected=1 will be returned for the sub-user associated with this user group. Example: user1
UserStatus	No	Yes	String	User status: Enabled, Disabled. Example: Enabled
UserType	No	Yes	String	User type. Manual: manually created; Synchronized: externally imported. Example: Manual
MaxResults	No	Yes	Int64	Maximum number of data entries per page. Value range: 1–100. Default value: 10. Example: 1
SortField	No	Yes	String	Sorting field, which currently only supports CreateTime. The default is the CreateTime field. Example: CreateTime
SortType	No	Yes	String	Sorting order. Desc: descending order; Asc: ascending order. It should be set together with SortField. Example: Desc
Offset	No	Yes	Int64	Pagination offset. Do not use it together with NextToken, prioritizing using NextToken. Example: 0

3. Output Parameters

Parameter name	Type	Description
Users	Array of UserInfo	User list. Example:View
NextToken	String	Token for querying the next page of returned results. This parameter is displayed only when IsTruncated is true. Example: sjdhdhw
IsTruncated	Bool	Whether the returned result is truncated. Valid values: true: truncated; false: not truncated. Example: true
TotalCounts	Int64	Total number of data entries that meet the request parameter conditions. Example: 1
MaxResults	Int64	Maximum number of data entries per page. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter.ParamError	
FailedOperation.IdentityCenterNotOpen	
FailedOperation.ZoneIdNotExist	
InvalidParameter.NextTokenInvalid	

UpdateUser

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

Modify user information

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateUser
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
NewLastName	No	Yes	String	Last name of the user. Example: John
NewDisplayName	No	Yes	String	Display name of the user. Example: John
NewDescription	No	Yes	String	User description. Example: description
NewEmail	No	Yes	String	Email address of the user. Example: John@example.com
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***

Parameter name	Required	Allow NULL	Type	Description
UserId	Yes	Yes	String	User ID. Example: u-34nesn3u
NewFirstName	No	Yes	String	First name of the user. Example: John

3. Output Parameters

Parameter name	Type	Description
UserInfo	UserInfo	User information Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.ManualUserNotUpdate	
FailedOperation.SynchronizedUserNotUpdate	
InvalidParameter.EmailAlreadyExists	
FailedOperation.ZoneIdNotExist	
FailedOperation.IdentityCenterNotOpen	
ResourceNotFound.UserNotExist	

UpdateUserStatus

1. Interface Description

Interface request domain name: cic.api3.convergecloud.com.

This API is used to modify the user status.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-11 12:17:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateUserStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2021-03-31
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ZoneId	Yes	Yes	String	Space ID. Example: z-2d8shd8***
UserId	Yes	Yes	String	User ID. Example: u-34nesn3u
NewUserStatus	Yes	Yes	String	User status. Valid values: Enabled, Disabled. Example: Enabled

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.ManualUserNotUpdate	
FailedOperation.SynchronizedUserNotUpdate	
FailedOperation.ZoneIdNotExist	
FailedOperation.IdentityCenterNotOpen	
ResourceNotFound.UserNotExist	

Data structure

UserInfo

User information

Referenced by the following interfaces: CreateUser, GetUser, ListUsers, UpdateUser

name	required	NULL allowed	type	description
UserStatus	no	no	String	User status: Enabled, Disabled. Example: Enabled
UserType	no	no	String	User type. Manual: manually created; Synchronized: externally imported. Example: Manual
UserId	no	no	String	User ID Example: u-34nesn3u
IsSelected	no	no	Bool	Whether selected Example: false
UserName	no	no	String	Queried username. Example: Alice
DisplayName	no	no	String	Display name of the user. Example: Alice
Description	no	no	String	User description. Example: description
Email	no	no	String	Email address of the user, which must be unique within the directory. Example: Alice@example.com
CreateTime	no	no	String	Creation time of the user. Example: 2025-01-03 12:12:23
UpdateTime	no	no	String	Modification time of the user. Example: 2025-01-03 12:12:23
FirstName	no	no	String	First name of the user. Example: Alice
LastName	no	no	String	Last name of the user. Example: Alice

RoleAssignmentInfo

Authorized member account information.

Referenced by the following interfaces: CreateRoleAssignment

name	required	NULL allowed	type	description
PrincipalId	no	no	String	ID of the object for CAM user synchronization. When the PrincipalType value is Group, the value is the ID of an Identity Center user group (g-). When the PrincipalType value is User, the value is the ID of an Identity Center user (u-). Example: u-xuec8dnd
PrincipalType	no	no	String	Type of the object for CAM user synchronization. Valid values: User: an Identity Center user. Group: an Identity Center user group. Example: User
TargetUin	no	no	Int64	UIN of the synchronized target account of the TCO. Example: 111111111111
TargetType	no	no	String	Type of the synchronized target account of the TCO. ManagerUin: admin account; MemberUin: member account. Example: MemberUin
RoleConfigurationId	no	no	String	Permission configuration ID. Example: rc-sixjtia

ZoneStatistics

CIC space statistics.

Referenced by the following interfaces: GetZoneStatistics

name	required	NULL allowed	type	description
RoleConfigurationSyncCount	no	no	Int64	Number of synchronized roles. Example: 1
UserQuota	no	no	Int64	User quota. Example: 20
GroupQuota	no	no	Int64	User group quota. Example: 20
RoleConfigurationQuota	no	no	Int64	Permission configuration quota. Example: 20
SystemPolicyPerRoleConfigurationQuota	no	no	Int64	System policy quota bound to the permission configuration. Example: 20
UserCount	no	no	Int64	Number of users. Example: 1
GroupCount	no	no	Int64	Number of user groups. Example: 1
RoleConfigurationCount	no	no	Int64	Number of permission configurations. Example: 1
UserProvisioningCount	no	no	Int64	Number of synchronized users. Example: 1

AccountUserProvisioning

Configuration information on a member account synchronized by a user.

Referenced by the following interfaces: ListAccountsForUserProvisioning

name	required	NULL allowed	type	description
Uin	no	yes	Int64	UIN of the synchronized target member account. Example: 111111111111
Name	no	yes	String	Name of the synchronized target member account. Example: member1
UserId	no	yes	String	User ID Example: u-34nesn3u
SyncSubUin	no	yes	String	UIN of the sub-account created during synchronization. Example: 2222222222222
SyncSubName	no	yes	String	Name of the sub-account created during synchronization. Example: sub_user

CreateUserInfo

Information on users created in batches.

Referenced by the following interfaces: BatchCreateUser

name	required	NULL allowed	type	description
UserName	yes	no	String	User name, which should be unique within the space and cannot be modified. It contains up to 64 characters, including digits, English letters, and special characters such as plus signs (+), equal signs (=), commas (,), periods (.), at signs (@), hyphens (-), and underscores (_). Example: Alice
FirstName	no	no	String	Last name of the user, which contains up to 64 characters. Example: Alice
LastName	no	no	String	First name of the user, which contains up to 64 characters. Example: Alice
DisplayName	no	no	String	Display name of the user, which contains up to 256 characters. Example: Alice
Description	no	no	String	User description, which contains up to 1024 characters. Example: description
Email	no	no	String	Email address of the user, which must be unique within the directory and contains up to 128 characters. Example: Alice@example.com
UserStatus	no	no	String	User status. Valid values: Enabled (default), Disabled. Example: Enabled

UserSyncProvisioning

CAM user synchronization information.

Referenced by the following interfaces: CreateUserSyncProvisioning

name	required	NULL allowed	type	description
Description	no	no	String	Description. Example: his is cam user
PrincipalId	no	no	String	ID of the object for CAM user synchronization. When the PrincipalType value is Group, the value is the ID of an Identity Center user group (g-). When the PrincipalType value is User, the value is the ID of an Identity Center user (u-). Example: u-xuec8dnd
PrincipalType	no	no	String	Type of the object for CAM user synchronization. Valid values: User: an Identity Center user. Group: an Identity Center user group. Example: User
TargetUin	no	no	Int64	UIN of the synchronized target account of the TCO. Example: 111111111111
DuplicationStrategy	no	no	String	Conflict policy. It indicates the handling policy for existence of a user with the same username when CIC users are synchronized to CAM. Valid values: KeepBoth: Keep both, that is, add the _cic suffix to the CIC user's username and then try to create a CAM user with the username when CIC users are synchronized to CAM and a user with the same username already exists in CAM; TakeOver: Replace, that is, directly replace the existing CAM user with the synchronized CIC user when CIC us Example: KeepBoth
DeletionStrategy	no	no	String	Deletion policy. It indicates the handling policy for CAM users already synchronized when the CAM user synchronization is deleted. Valid values: Delete: Delete the CAM users already synchronized from CIC to CAM when the CAM user synchronization is deleted; Keep: Keep the CAM users already synchronized from CIC to CAM when the CAM user synchronization is deleted. Example: Delete
TargetType	no	no	String	Type of the synchronized target account of the TCO. ManagerUin: admin account; MemberUin: member account. Example: MemberUin

SAMLIdPCertificate

SAML signing certificate information.

Referenced by the following interfaces: ListExternalSAMLIdPCertificates

name	required	NULL allowed	type	description
SerialNumber	no	no	String	Certificate serial number. Example: 134759421819****
PublicKey	no	no	String	Public key certificate in PEM format (Base64 encoded). Example: nMIBIjCCAV***
SignatureAlgorithm	no	no	String	Signature algorithm of the certificate. Example: SHA256withRSA***
NotAfter	no	no	String	Expiration time of the certificate. Example: 2030-06-23 07:09:11
NotBefore	no	no	String	Creation time of the certificate. Example: 2023-06-23 07:09:11
Subject	no	no	String	Certificate subject. Example: 5.6.54.22.1.9.1=#dj39dj39e3w9rm3e2e3****,CN=dev-xxxxxx,OU=SSOProvider,O=Okta
X509Certificate	no	no	String	X509 certificate in PEM format. Example: nMIBIjCCAV****
Issuer	no	no	String	Certificate issuer. Example: 5.6.54.22.1.9.1=#dj39dj39e3w9rm3e2e3****,CN=dev-xxxxxx,OU=SSOProvider,O=Okta
Version	no	no	Int64	Certificate version. Example: 1
CertificateId	no	no	String	Certificate ID. Example: dp-c-2jd8923je29****

GroupIdAndUserId

User group ID and user IDs.

Referenced by the following interfaces: BatchAddUserToGroup, BatchRemoveUserFromGroup

name	required	NULL allowed	type	description
GroupId	yes	no	String	User Group ID Example: g-sd8hd8sdno***
UserId	yes	no	String	User ID Example: u-34nesn3u

UserProvisioning

User synchronization information.

Referenced by the following interfaces: GetUserSyncProvisioning, ListUserSyncProvisionings

name	required	NULL allowed	type	description
TargetName	no	no	String	Name of the target account of the TCO. Example: user1
DuplicationStrategy	no	no	String	Conflict policy. It indicates the handling policy for existence of a user with the same username when CIC users are synchronized to CAM. Valid values: KeepBoth: Keep both, that is, add the _cic suffix to the CIC user's username and then try to create a CAM user with the username when CIC users are synchronized to CAM and a user with the same username already exists in CAM; TakeOver: Replace, that is, directly replace the existing CAM user with the synchronized CIC user when CIC us Example: KeepBoth
DeletionStrategy	no	no	String	Deletion policy. It indicates the handling policy for CAM users already synchronized when the CAM user synchronization is deleted. Valid values: Delete: Delete the CAM users already synchronized from CIC to CAM when the CAM user synchronization is deleted; Keep: Keep the CAM users already synchronized from CIC to CAM when the CAM user synchronization is deleted. Example: Delete
CreateTime	no	no	String	Creation time. Example: 2025-01-03 12:12:23
UpdateTime	no	no	String	Update time. Example: 2025-01-03 12:12:23
UserProvisioningId	no	no	String	CAM user synchronization status. Valid values: Enabled: CAM user synchronization is enabled. Disabled: CAM user synchronization is disabled. Example: up-sjiwwBois
Status	no	no	String	CAM user synchronization status. Valid values: Enabled: CAM user synchronization is enabled. Disabled: CAM user synchronization is disabled. Example: Enabled
PrincipalName	no	no	String	Name of the object for CAM user synchronization. When the PrincipalType value is Group, the value is the name of an Identity Center user group. When the PrincipalType value is User, the value is the name of an Identity Center user. Example: user1
PrincipalType	no	no	String	Type of the object for CAM user synchronization. Valid values: User: an Identity Center user. Group: an Identity Center user group. Example: User
TargetUin	no	no	Int64	UIN of the target account of the TCO. Example: 111111111111
TargetType	no	no	String	Type of the synchronized target account of the TCO. ManagerUin: admin account; MemberUin: member account. Example: MemberUin
Description	no	no	String	Description. Example: description
PrincipalId	no	no	String	ID of the object for CAM user synchronization. When the PrincipalType value is Group, the value is the ID of an Identity Center user group (g-). When the PrincipalType value is User, the value is the ID of an Identity Center user (u-). Example: u-xuec8dnd

UserProvisioningsTask

Status information of the user synchronization task.

Referenced by the following interfaces: CreateUserSyncProvisioning, DeleteUserSyncProvisioning

name	required	NULL allowed	type	description
PrincipalType	no	no	String	Type of the object for CAM user synchronization. Valid values: User: an Identity Center user. Group: an Identity Center user group. Example: User
PrincipalName	no	no	String	User name or user group name. Example: user1
DeletionStrategy	no	no	String	Deletion policy: Delete, Keep. Example: Delete
TaskId	no	no	String	Task ID. Example: t-xBjd5983e****
TaskType	no	no	String	Task type. StartProvisioning: Start the user synchronization; DeleteProvisioning: Delete the user synchronization. Example: CreateRoleAssignment
TaskStatus	no	no	String	Task status. InProgress: The task is in progress; Failed: The task failed; Success: The task successful. Example: InProgress
UserProvisioningId	no	no	String	User synchronization ID. Example: up-sjiwwBois
TargetUin	no	no	Int64	UIN of the authorized target account of the TCO. Example: 111111111111
TargetType	no	no	String	Type of the synchronized target account of the TCO. ManagerUin: admin account; MemberUin: member account. Example: MemberUin
PrincipalId	no	no	String	ID of the object for CAM user synchronization. Valid values: When the PrincipalType value is Group, the value is the ID of an Identity Center user group (g-). When the PrincipalType value is User, the value is the ID of an Identity Center user (u-). Example: u-xuec8dnd
DuplicationStrategy	no	no	String	Conflict policy. KeepBoth: Keep both; TakeOver: Replace. Example: KeepBoth

SAMLIdentityProviderConfiguration

SAML identity provider configuration information.

Referenced by the following interfaces: GetExternalSAMLIdentityProvider

name	required	NULL allowed	type	description
LoginUrl	no	no	String	IdP login URL. Example: https://dev-xxxxx
CreateTime	no	no	String	Creation time. Example: 2025-01-03 12:12:23
UpdateTime	no	no	String	Update time. Example: 2025-01-03 12:12:23
EntityId	no	no	String	IdP identifier. Example: http://www.***.com
SSOStatus	no	no	String	SSO enabling status. Valid values: Enabled, Disabled (default). Example: Enbaled
EncodedMetadataDocument	no	no	String	IdP metadata document (Base64 encoded). Example: PD94bWwgdmVyc2lvbj0****
CertificateIds	no	no	Array of String	X509 certificate ID. Example: dp-c-2jd8921je29****

GroupInfo

User group information.

Referenced by the following interfaces: CreateGroup, GetGroup, ListGroups, UpdateGroup

name	required	NULL allowed	type	description
GroupId	no	no	String	User group ID. Example: g-sd8hd8sdno***
MemberCount	no	no	Int64	Number of group members. Example: 1
IsSelected	no	no	Bool	If the input parameter FilterUsers is provided, return true when the user is in the user group; otherwise, return false. Example: true
GroupName	no	no	String	User group name. Example: group_name
Description	no	no	String	User group description. Example: description
CreateTime	no	no	String	Creation time of the user group. Example: 2025-01-03 12:12:23
GroupType	no	no	String	User group type. Manual: manually created; Synchronized: externally imported. Example: Manual
UpdateTime	no	no	String	Modification time of the user group. Example: 2025-01-03 12:12:23

SAMLServiceProvider

SAML service provider information.

Referenced by the following interfaces: GetZoneSAMLServiceProviderInfo

name	required	NULL allowed	type	description
EntityId	no	no	String	https://XXX/saml/sp/z-sjw8ensa Example: https://XXX/saml/sp/z-sjw8*
ZoneId	no	no	String	Space ID. Example: z-2d8bhd8****
EncodedMetadataDocument	no	no	String	SP metadata document (Base64 encoded). Example: JTNDJTNGeG1sJTIwdmVyc2lvbiUzRCUyMSUyMGVuY29kaW5nJTNEJ***
AcsUrl	no	no	String	SP ACS URL. Example: https://XXX.com/saml/acs/swede-22a20dc2-x2je6****

JoinedGroups

User group joined by the user.

Referenced by the following interfaces: ListJoinedGroupsForUser

name	required	NULL allowed	type	description
GroupName	no	no	String	User group name. Example: group_name
Description	no	no	String	User group description. Example: description
GroupId	no	no	String	User group ID. Example: g-sd8hd8sdno***
GroupType	no	no	String	User group type. Valid values: Manual: manually created; Synchronized: externally synchronized. Example: Manual
JoinTime	no	no	String	Time of joining the user group. Example: 2025-01-03 12:12:23

RoleConfiguration

CIC permission configuration.

Referenced by the following interfaces: CreateRoleConfiguration

name	required	NULL allowed	type	description
RelayState	no	no	String	Initial access page. It indicates the initial access page URL when CIC users use the access configuration to access member accounts. Example: https://XXX
CreateTime	no	no	String	Creation time of the permission configuration. Example: 2025-01-03 12:12:23
UpdateTime	no	no	String	Update time of the permission configuration. Example: 2025-01-03 12:12:23
IsSelected	no	no	Bool	If the input parameter FilterTargets is provided, check whether the member account has been configured with permissions. If configured, return true; otherwise, return false. Example: false

name	required	NULL allowed	type	description
RoleConfigurationId	no	no	String	Permission configuration ID. Example: rc-sisjdia
RoleConfigurationName	no	no	String	Permission configuration name. Example: conf1
Description	no	no	String	Permission configuration description. Example: description
SessionDuration	no	no	Int64	Session duration. The maximum time a session is maintained when an Identity Center user accesses a member account by using the access configuration. Unit: seconds. Example: 60

TaskStatus

Task status information.

Referenced by the following interfaces: GetProvisioningTaskStatus

name	required	NULL allowed	type	description
FailureReason	no	no	String	Task failure cause. Note: This parameter is displayed only when the Status value is Failed. Example: Failed
Status	no	no	String	Task status. Valid values: InProgress: The task is being executed; Success: The task executed successfully; Failed: The task execution failed. Example: InProgress
TaskId	no	no	String	Task ID. Example: t-sdjsf983n****
TaskType	no	no	String	Task type. Valid values: ProvisionRoleConfiguration: deploy permission configuration; DeprovisionRoleConfiguration: Cancel permission configuration deployment; CreateRoleAssignment: Assign permissions for a member account; DeleteRoleAssignment: Remove permissions from a member account. Example: CreateRoleAssignment

TaskInfo

Task status information.

Referenced by the following interfaces: CreateRoleAssignment

name	required	NULL allowed	type	description
TaskId	no	no	String	Task ID. Example: t-sdjsf983n****
RoleConfigurationId	no	no	String	Permission configuration ID. Example: rc-sisjdia
PrincipalId	no	no	String	Identity ID for the user authorization. If the identity type is CIC user, it is the user ID; if the identity type is user group, it is the user group ID. Example: u-xaec8dnd
PrincipalType	no	no	String	Identity type for the user authorization. User: CIC user; Group: CIC user group. Example: User
TaskType	no	no	String	Task type. Example: CreateRoleAssignment
Status	no	no	String	InProgress: The task is being executed; Success: The task executed successfully; Failed: The task execution failed. Example: InProgress
RoleConfigurationName	no	no	String	Permission configuration name. Example: conf1
TargetUin	no	no	Int64	UIN of the authorized target member account. Example: 11111111111
TargetType	no	no	String	Type of the synchronized target account. ManagerUin: admin account; MemberUin: member account. Example: MemberUin
FailureReason	no	yes	String	Failure reason Example: Failed

GroupMembers

User information

Referenced by the following interfaces: ListGroupMembers

name	required	NULL allowed	type	description
UserType	no	no	String	User type. Manual: manually created; Synchronized: externally imported. Example: Manual
UserId	no	no	String	User ID Example: u-34nesn3u
JoinTime	no	no	String	Time when the user joins the user group. Example: 2025-01-03 12:12:23
UserName	no	no	String	Queried username. Example: Alice
DisplayName	no	no	String	Display name of the user. Example: Alice
Description	no	no	String	User description. Example: description
Email	no	no	String	Email address of the user, which must be unique within the directory. Example: Alice@example.com
UserStatus	no	no	String	User status: Enabled, Disabled. Example: Enabled

SCIMCredential

SCIM key.

Referenced by the following interfaces: ListSCIMCredentials

name	required	NULL allowed	type	description
CreateTime	no	no	String	Creation time of a SCIM key. Example: 2025-01-03 12:12:23
ExpireTime	no	no	String	Expiration time of a SCIM key. Example: 2025-01-03 12:12:23
ZoneId	no	no	String	Space ID, which starts with the z- prefix, followed by 12 random digits/lowercase letters. Example: z-2d8xhd8***
Status	no	no	String	SCIM key status. Enabled: enabled. Disabled: disabled. Example: Enabled
CredentialId	no	no	String	SCIM key ID, which starts with the scimcred- prefix, followed by 12 random digits/lowercase letters. Example: scimcred-8g****
CredentialType	no	no	String	SCIM key type. Example: BearerToken

ErrorCode

Feature Description

If there is an Error field in the response, it means that the API call failed. For example:

```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```

Code in Error indicates the error code, and Message indicates the specific information of the error.

Error Code List

Common Error Codes

Error codes	Description
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	Key does not exist. Check if the key has been deleted or disabled in the console, and if not, check if the key is correctly entered. Note that whitespaces should not exist before or after the key.
AuthFailure.SignatureExpire	Signature expired. Timestamp and server time cannot differ by more than five minutes. Please ensure your current local time matches the standard time.
AuthFailure.SignatureFailure	Invalid signature. Signature calculation error. Please ensure you've followed the signature calculation process described in the Signature API documentation.
AuthFailure.TokenFailure	Token error.

Error codes	Description
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	HTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

Service Error Codes

Error codes	Description
InvalidParameter.NamePasswordNotExist	

Error codes	Description
FailedOperation.AudienceFormatError	
FailedOperation.RoleConfigurationProvisioningStatusError	
InvalidParameter.ConfigurationNameFormatError	
InvalidParameter.SPEntityIDError	
FailedOperation.ManualGroupNotUpdate	
FailedOperation.ManualGroupNotDelete	
FailedOperation.MetadataCosParsingFailed	
FailedOperation.RoleConfigurationAuthorizationAlreadyExist	
InvalidParameter.UsernameFormatError	
FailedOperation.DecodeMetadataDocumentFailed	
ResourceNotFound.UserNotExist	
FailedOperation.AddUserOverLimit	
FailedOperation.IdentityCenterNotOrganizationManager	
FailedOperation.JWTClaimsFailed	
FailedOperation.SynchronizedUserNotUpdate	
InvalidParameter.RequestParamUserNameRepeat	
FailedOperation.RoleConfigurationAuthorizationOverLimit	
FailedOperation.ConfigurationOverUpperLimit	
FailedOperation.UserForbidLogin	
FailedOperation.IDPMetadataVerifyFailed	
ResourceNotFound.RoleConfigurationProvisioningNotFound	
FailedOperation.ZoneIdNotExist	
LimitExceeded.RemoveUserFromGroupLimitExceeded	
InvalidParameter.UsernameAlreadyExists	
FailedOperation.UserProvisioningOverLimit	

Error codes	Description
InvalidParameter.SAMLResponseNotExist	
InvalidParameter.ParamError	
LimitExceeded.AddUserToGroupLimitExceeded	
FailedOperation.UploadMetadataFailed	
FailedOperation.OrganizationMemberNotExist	
InvalidParameter.ScimCredentialNotFound	
FailedOperation.IdentityCenterOrganizationNotOpen	
FailedOperation.SynchronizedGroupNotUpdate	
InvalidParameterValue.X509CertificateFormatError	
FailedOperation.GroupUserCountOverUpperLimit	
FailedOperation.XMLDataUnmarshalFailed	
InvalidParameter.GroupUserNotExist	
InvalidParameter.GroupNotExist	
FailedOperation.SSoStatusEnableNotClearIdentityProvider	
FailedOperation.IdentityCenterNotEnterpriseAuth	
FailedOperation.IdentityProviderNotConfigured	
ResourceNotFound.SAMLServiceProviderNotFound	
ResourceNotFound.UserProvisioningNotFound	
FailedOperation.ParsePrivateKeyError	
FailedOperation.DBOperationError	
FailedOperation.TokenExpired	
FailedOperation.UserProvisioningFailed	
ResourceNotFound.SAMLIdentityProviderNotFound	
FailedOperation.JWTSignFailed	
FailedOperation.SynchronizedGroupNotAddUser	

Error codes	Description
FailedOperation.UserProvisioningAlreadyExists	
InvalidParameter.EmailAlreadyExists	
FailedOperation.DeleteGroupNotAllowExistUser	
InvalidParameter.UserAlreadyExistsGroup	
ResourceNotFound.X509CertificateNotFound	
FailedOperation.GroupOverUpperLimit	
FailedOperation.ManualUserNotUpdate	
InvalidParameter.ConfigurationNameAlreadyExists	
FailedOperation.SynchronizedGroupNotRemoveUser	
FailedOperation.SAMLServiceProviderCreateFailed	
FailedOperation.SAMLMetadataDocumentGetFailed	
FailedOperation.JWTVerifyFailed	
FailedOperation.SynchronizedGroupNotDelete	
InvalidParameter.UserScimCredentialStatusError	
InvalidParameterValue.ZoneNameFormatError	
InvalidParameter.RequestParamEmailRepeat	
InvalidParameter.GroupNameFormatError	
FailedOperation.GroupTypeUserTypeNotMatch	
LimitExceeded.ScimCredentialLimitExceeded	
FailedOperation.AESCryptoFailed	
InvalidParameter.RoleConfigurationNotExist	
FailedOperation.X509CertificateAlreadyExist	
InvalidParameterValue.LoginTypeInvalid	
FailedOperation.X509CertificateParsingFailed	
FailedOperation.IdentityCenterNotAuth	

Error codes	Description
LimitExceeded.CreateUserSyncProvisioningLimitExceeded	
FailedOperation.SAMLResponseVerifyFailed	
FailedOperation.IdentityCenterNotOpen	
LimitExceeded.CreateUserLimitExceeded	
ResourceNotFound.ServiceRoleNotExist	
FailedOperation.AddUserToGroupOverLimitPerRequest	
ResourceNotFound.UserProvisioningTaskNotFound	
LimitExceeded.CreateRoleAssignmentLimitExceeded	
InvalidParameter.NextTokenInvalid	
InvalidParameter.GroupUserAlreadyExists	
InternalError	
FailedOperation.SynchronizedUserNotDelete	
FailedOperation.RoleConfigurationAuthorizationExist	
FailedOperation.AccountPasswordLoginNotSupport	
FailedOperation.UserProvisioningExists	
InvalidParameter.GroupNameAlreadyExists	
FailedOperation.UserOverUpperLimit	
InvalidParameterValue.IdentityCenterZoneNameAlreadyExist	
FailedOperation.IdentityCenterAlreadyOpen	
InvalidParameter.ScimSyncStatusError	
FailedOperation.GenSamlResponseError	
InvalidParameterValue.SSoStatusInvalid	
FailedOperation.UserAddGroupCountOverUpperLimit	
FailedOperation.ScimCredentialGenerateError	
FailedOperation.ManualUserNotDelete	

Error codes	Description
FailedOperation.PrivateKeyDecodeError	

Organization Account Management(organization) version(2022-05-08) API overview

API version

V3

Department and Member Management APIs

Interface name	Interface function
AddOrganizationMemberEmail	AddOrganizationMemberEmail
CheckAccountDelete	CheckAccountDelete
CreateOrganizationMember	CreateOrganizationMember
DeleteAccount	DeleteAccount
DeleteOrganizationMembers	DeleteOrganizationMembers
DescribeOrganizationMemberEmailBind	DescribeOrganizationMemberEmailBind
SendOrgMemberAccountBindEmail	SendOrgMemberAccountBindEmail
UpdateOrganizationMember	UpdateOrganizationMember
UpdateOrganizationMemberEmailBind	UpdateOrganizationMemberEmailBind

Financial Overview APIs

Interface name	Interface function
DescribeOrganizationFinancialByMember	DescribeOrganizationFinancialByMember
DescribeOrganizationFinancialByMonth	DescribeOrganizationFinancialByMonth

Interface name	Interface function
DescribeOrganizationFinancialByProduct	DescribeOrganizationFinancialByProduct

Organization Management Policy APIs

Interface name	Interface function
ListPolicies	ListPolicies
ListPoliciesForTarget	ListPoliciesForTarget

Organization Settings APIs

Interface name	Interface function
CreateOrganization	CreateOrganization
DeleteOrganization	DeleteOrganization
QuitOrganization	QuitOrganization

Unified Member Login APIs

Interface name	Interface function
CreateOrganizationIdentity	CreateOrganizationIdentity
CreateOrganizationMemberAuthIdentity	CreateOrganizationMemberAuthIdentity
CreateOrganizationMembersPolicy	CreateOrganizationMembersPolicy
DeleteOrganizationIdentity	DeleteOrganizationIdentity
DeleteOrganizationMemberAuthIdentity	DeleteOrganizationMemberAuthIdentity
DeleteOrganizationMembersPolicy	DeleteOrganizationMembersPolicy
DescribeOrganizationMemberAuthIdentities	DescribeOrganizationMemberAuthIdentities
DescribeOrganizationMemberPolicies	DescribeOrganizationMemberPolicies

Interface name	Interface function
ListOrganizationIdentity	ListOrganizationIdentity
UpdateOrganizationIdentity	UpdateOrganizationIdentity

CallingMethod signaturev1

Converge Cloud authenticates each access request, i.e. each request needs to include authentication information (Signature) in the common parameters to verify the identity of the requester.
The Signature is generated by the security credentials which include SecretId and SecretKey. If you don't have the security credentials yet, go to the API Key page to apply for them; otherwise, you cannot invoke the API.

1. Applying for Security Credentials

Before using the API for the first time, go to the API Key page to apply for security credentials.
Security credentials consist of SecretId and SecretKey:

- SecretId is used to identify the API requester.
- SecretKey is used to encrypt the signature string and verify it on the server.
- You must keep your security credentials private and avoid disclosure.

You can apply for the security credentials through the following steps:

1. Log in to the Converge Cloud Console.
2. Go to the Cloud API Key page.
3. On the API Key Management page, click Create Key to create a SecretId/SecretKey pair.

Note: Each account can have up to two pairs of SecretId/SecretKey.

2. Generating a Signature

With the SecretId and SecretKey, a signature can be generated. The following describes how to generate a signature:

Assume that the SecretId and SecretKey are:

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

Note: This is just an example. For actual operations, please use your own SecretId and SecretKey.

Take the Cloud Virtual Machine's request to view the instance list (DescribeInstances) as an example. When

you invoke this API, the request parameters may be as follows:

Parameter name	Description	Parameter value
Action	Method name	DescribeInstances
SecretId	Key ID	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	Current timestamp	1465185768
Nonce	Random positive integer	11886
Region	Region where the instance is located	luzon
InstanceIds.0	ID of the instance to query	ins-09dx96dg
Offset	Offset	0
Limit	Allowed maximum output	20
Version	API version number	2017-03-12

2.1. Sorting Parameters

First, sort all the request parameters in an ascending lexicographical order (ASCII code) by their names. Notes: (1) Parameters are sorted by their names instead of their values; (2) The parameters are sorted based on ASCII code, not in an alphabetical order or by values. For example, InstanceIds.2 should be arranged after InstanceIds.12. You can complete the sorting process using a sorting function in a programming language, such as the ksort function in PHP. The parameters in the example are sorted as follows:

```
{
    'Action' : 'DescribeInstances',
    'InstanceIds.0' : 'ins-09dx96dg',
    'Limit' : 20,
    'Nonce' : 11886,
    'Offset' : 0,
    'Region' : 'luzon',
    'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
    'Timestamp' : 1465185768,
    'Version': '2017-03-12',
}
```

When developing in another programming language, you can sort these sample parameters and it will work as long as you obtain the same results.

2.2. Concatenating a Request String

This step generates a request string.
Format the request parameters sorted in the previous step into the form of "parameter name"="parameter value". For example, for the Action parameter, its parameter name is "Action" and its parameter value is "DescribeInstances", so it will become Action=DescribeInstances after formatted.
Note: The "parameter value" is the original value but not the value after URL encoding.

Then, concatenate the formatted parameters with "&". The resulting request string is as follows:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. Concatenating the Signature Original String

This step generates a signature original string.
The signature original string consists of the following parameters:

1. HTTP method: POST and GET modes are supported, and GET is used here for the request. Please note that the method name should be in all capital letters.
2. Request host: the domain name of the request to view the list of instances (DescribeInstances) is cvm.convergecloud.com. The actual request domain name varies by the module to which the API belongs. For more information, see the instructions of the specific API.
3. Request path: The request path in the current version of Cloud API is fixed to / .
4. Request string: the request string generated in the previous step.

The concatenation rule of the signature original string is: Request method + request host + request path + ? + request string

The concatenation result of the example is:

```
GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. Generating a Signature String

This step generates a signature string.
First, use the HMAC-SHA1 algorithm to sign thesignature original stringobtained in the previous step, and then encode the generated signature using Base64 to obtain the final signature.

The specific code is as follows with the PHP language being used as an example:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit
=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPL
E&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

The final signature is:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

When developing in another programming language, you can sign and verify the original in the example above and it works as long as you get the same results.

3. Encoding a Signature String

The generated signature string cannot be directly used as a request parameter and must be URL encoded.

For example, if the signature string generated in the previous step is EliP9YW3pW28FpsEdkXt/+WcGeI= , the final signature string request parameter (Signature) is EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d, which will be used to generate the final request URL.

**Note: If your request method is GET, or the request method is POST and the Content-Type is application/x-www-form-urlencoded, then all the request parameter values need to be URL encoded (except the parameter key and the symbol of =) when sending the request. Non-ASCII characters need to be encoded with UTF-8 before URL encoding. **

Note: The network libraries of some programming languages automatically URL encode all parameters, in which case there is no need to URL encode the signature string; otherwise, two rounds of URL encoding will cause the signature to fail.

Note: Other parameter values also need to be encoded using RFC 3986. Use %XY in percent-encoding for special characters such as Chinese characters, where "X" and "Y" are hexadecimal characters (0-9 and uppercase A-F), and using lowercase will cause an error.

4. Signature Failure

The following situational error codes for signature failure may occur. Please resolve the errors accordingly.

Error code	Error description
AuthFailure.SignatureExpire	The signature is expired

Error code	Error description
AuthFailure.SecretIdNotFound	The key does not exist
AuthFailure.SignatureFailure	Signature error
AuthFailure.TokenFailure	Token error
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type)

5. Signature Demo

When calling API 3.0, you are recommended to use the corresponding Converge Cloud SDK 3.0, Swhich encapsulates the signature process, enabling you to focus on only the specific APIs provided by the product when developing. See SDK Center for more information. Currently, the following programming languages are supported:

- Python
- Java
- PHP
- Go
- Node

To further explain the signing process, we will use a programming language to implement the process described above. The request domain name, API and parameter values in the sample are used here. This goal of this example is only to provide additional clarification for the signature process, please see the SDK for actual usage.

The final output URL might be: https://cvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

Note: The key in the example is fictitious, and the timestamp is not the current time of the system, so if this URL is opened in the browser or called using commands such as curl, an authentication error will be returned: Signature expired. In order to get a URL that can work properly, you need to replace the SecretId and SecretKey in the example with your real credentials and use the current time of the system as the Timestamp.

Note: In the example below, even if you use the same programming language, the order of the parameters in the URL may be different for each execution. However, the order does not matter, as long as all the parameters are included in the URL and the signature is calculated correctly.

Note: The following code is only applicable to API 3.0. It cannot be directly used in other signature processes. Even with an older API, signature calculation errors may occur due to the differences in details. Please refer to the corresponding documentation.

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class CloudAPIDemo {
    private final static String CHARSET = "UTF-8";

    public static String sign(String s, String key, String method) throws Exception {
        Mac mac = Mac.getInstance(method);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
        mac.init(secretKeySpec);
        byte[] hash = mac.doFinal(s.getBytes(CHARSET));
        return DatatypeConverter.printBase64Binary(hash);
    }

    public static String getStringToSign(TreeMap<String, Object> params) {
        StringBuilder s2s = new StringBuilder("GETcvm.convergecloud.com/?");
        // When signing, the parameters need to be sorted in lexicographical order. TreeMap is used here
to guarantee the correct order.
        for (String k : params.keySet()) {
            s2s.append(k).append("=").append(params.get(k).toString()).append("&");
        }
        return s2s.toString().substring(0, s2s.length() - 1);
    }

    public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException
{
        StringBuilder url = new StringBuilder("https://cvm.convergecloud.com/?");
        // There is no requirement for the order of the parameters in the actual request URL.
        for (String k : params.keySet()) {
            // The request string needs to be URL encoded. As the Key is all in English letters, only the valu
e is URL encoded here.
            url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).app
end("&");
        }
        return url.toString().substring(0, url.length() - 1);
```

```
    }

    public static void main(String[] args) throws Exception {
        TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap enables automati
c sorting
        // A random number should be used when actually calling, for example: params.put("Nonce", new
Random().nextInt(java.lang.Integer.MAX_VALUE));
        params.put("Nonce", 11886); // Common parameter
        // The current time of the system should be used when actually calling, for example:   params.put
("Timestamp", System.currentTimeMillis() / 1000);
        params.put("Timestamp", 1465185768); // Common parameter
        params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // Common parameter
        params.put("Action", "DescribeInstances"); // Common parameter
        params.put("Version", "2017-03-12"); // Common parameter
        params.put("Region", "luzon"); // Common parameter
        params.put("Limit", 20); // Business parameter
        params.put("Offset", 0); // Business parameter
        params.put("InstanceIds.0", "ins-09dx96dg"); // Business parameter
        params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE
", "HmacSHA1")); // Common parameter
        System.out.println(getUrl(params));
    }
}
```

Python

Note: If running in a Python 2 environment, the following requests dependency package must be installed first: pip install requests .

```
# -*- coding: utf8 -*-
import base64
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
    s = method + endpoint + "/?"
    query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
    return s + query_str

def sign_str(key, s, method):
```

```
    hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
    return base64.b64encode(hmac_str)

if __name__ == '__main__':
    endpoint = "cvm.convergecloud.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'luzon',
        'SecretId' : secret_id,
        'Timestamp' : 1465185768, # int(time.time())
        'Version': '2017-03-12'
    }
    s = get_string_to_sign("GET", endpoint, data)
    data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
    print(data["Signature"])
    # n actual invocation would occur here, which may incur fees after success
    # resp = requests.get("https://" + endpoint, params=data)
    # print(resp.url)
```

signaturev3

Converge Cloud The API will authenticate each access request, meaning that each request must include signature information (Signature) in the public request parameters to verify the requester's identity.
The signature information is generated by the security credentials, which include SecretId and SecretKey . If the user does not have security credentials, please apply for them on the Cloud API Key page, otherwise they cannot call the Cloud API interfaces.

1. Apply for security credentials.

Before using the Cloud API for the first time, please go to the Cloud API Key page to apply for a security credential.
Security credentials include SecretId and SecretKey:

- SecretId The security credentials are used to identify the identity of the API caller.
- SecretKey The secret key is used to encrypt and sign the string for server-side verification of the signature.
- Users must strictly protect their security credentials and avoid disclosure them.

The specific steps to apply for security credentials are as follows:

1. Log in to Converge Cloud Administration Center Console
2. Go to the console page for cloud API keys
3. On the Cloud API Key page, click New to create a pair of SecretId/SecretKey

Note: Developer accounts can have up to two pairs SecretId / SecretKey.

2. TC3-HMAC-SHA256 signature method

Note: For GET method, only Content-Type: application/x-www-form-urlencoded protocol format is supported. For POST method, Content-Type: application/json and Content-Type: multipart/form-data are currently supported. By default, all business interfaces are supported in json format. Only specific business interfaces are supported in multipart format. In this case, the interface cannot be called in json format. Refer to the specific business interface document description.

The following takes Cloud Virtual Machine querying Region-1 instance list as an example to introduce the signature calculation process step by step. We only use two parameters for the query instance list: Limit and Offset, called using the GET method.

Assume that the SecretId and SecretKey of the user are AKIDz 8krbsJ 5yKBZQpn 74WFkmLPx 3EXAMPLE and Gu 5t9xGARNpq 86cd 98joQYCN3EXAMPLE, respectively.

2.1. splice specification request string

Concatenate CanonicalRequest strings in the following format:

```
CanonicalRequest =
  HTTPRequestMethod + '\n' +
  CanonicalURI + '\n' +
  CanonicalQueryString + '\n' +
  CanonicalHeaders + '\n' +
  SignedHeaders + '\n' +
  HashedRequestPayload
```

- HTTPRequestMethod: HTTP request methods (GET, POST), GET in this example;
- CanonicalURI: URI parameter, API 3.0 fixed to forward slash (/);
- CanonicalQueryString: Query string in the URL that initiates the HTTP request. For POST requests, it is fixed as an empty string. For GET requests, it is the question mark (?) in the URL. The following string content, this example value is: Limit=10&Offset=0. Note: CanonicalQueryString needs to be URL encoded.
- CanonicalHeaders: The header information of participating signature, at least including host and content-type, can also be added with customized header to improve the uniqueness and security of its own request. Splicing rules: 1) head key and value are uniformly converted to lowercase, and the first and last spaces are removed, and spliced according to the format of key:value\n;2) multiple heads are spliced according to the dictionary sorting of head key (lowercase). In this example: content-type: application/x-www-form-urlencoded\nhost: cvm.convergecloud.com\n
- SignedHeaders: The header information involved in the signature indicates which headers participate in the signature of this request, and the header content contained in CanonicalHeaders is one-to-one corresponding. content-type and host are required headers. constructed as: 1) The head key is uniformly converted to lowercase; 2) Multiple header keys (lowercase) are concatenated according to dictionary sorting and separated by semicolons (;). In this case: content-type;host
- HashedRequestPayload: The hash value of the request body, calculated as Lowercase(HexEncode(Hash.SHA256(RequestPayload))), SHA256 hash the entire payload of the HTTP request body, then hexadecimal encoding, and finally converting the encoding string to lowercase letters. Note: For GET requests, RequestPayload is fixed as an empty string. For POST requests, RequestPayload is the payload of the HTTP request body.

According to the above rules, the resulting canonical request string in the example is as follows (for clarity, \nnewlines are replaced by a new line printed separately):

```
GET
```

```
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.convergecloud.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. Concatenate the string to be signed

Concatenate the string to be signed in the following format:

```
StringToSign =
  Algorithm + \n +
  RequestTimestamp + \n +
  CredentialScope + \n +
  HashedCanonicalRequest
```

- Algorithm: Signature algorithm, currently fixed as TC3-HMAC-SHA256;
- RequestTimestamp: Request timestamp, i.e. the X-TC-Timestamp value of the request header. The request in the example above is 1539084154;
- CredentialScope: Credential range in the format Date/service/tc3_request, containing date, requested service and termination string (tc3_request). **Date is the date of UTC standard time, the value needs to be consistent with UTC standard time converted by common parameter X-TC-Timestamp **;service is the product name, which must be consistent with the product domain name called, such as cvm. The above example request, the value is 2018-10-09/cvm/tc3_request;
- HashedCanonicalRequest: The hash value of the canonical request string obtained by concatenating the above steps is calculated by Lowercase(HexEncode(Hash.SHA256(CanonicalRequest))).

note:

> 1. Date must be calculated from timestamp X-TC-Timestamp and time zone UTC+0. Adding local time zone information to the system, such as East Zone 8, will cause calls to succeed during the day and night, but calls to fail in the early hours of the morning. Assuming the timestamp is 1551113065, the time in the East Eight District is 2019-02-26 00:44:25, but the calculated Date with UTC+0 should be 2019-02-25 instead of 2019-02-26.
> 2. Timestamp must be the current system time and ensure that the system time and standard time are synchronized. If the difference exceeds five minutes, it will fail. If it is not synchronized with the standard time for a long time, it may cause the request to fail after running for a period of time (return signature expiration error).

According to the above rules, the string to be signed in the example is as follows (for clarity,\nnewlines are

replaced by new lines printed):

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. calculate the signature

1. Compute the derived signature key, pseudocode as follows

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey: Original SecretKey;
- Date: That is, the Date field information in Credential, as shown in the example above, is 2018-10-09.;
- Service: That is, the Service field information in Credential, as shown in the example above, is cvm;

2. Calculate the signature, pseudocode as follows

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning: That is, the derivative signature key calculated above;
- StringToSign: That is, the character string to be signed calculated in step 2;

2.4. Splicing Authorization

Splice as follows Authorization:

```
Authorization =
    Algorithm + ' ' +
    'Credential=' + SecretId + '/' + CredentialScope + ', ' +
    'SignedHeaders=' + SignedHeaders + ', '
    'Signature=' + Signature
```

- Algorithm: Signature method, fixed as TC3-HMAC-SHA256;
- SecretId: SecretId in key pair;
- CredentialScope: See above, Scope of Voucher;
- SignedHeaders: See above, header information for participating signatures;
- Signature: signature value

According to the above rules, the values obtained in the example are:

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

The final complete invocation information is as follows:

```
https://cvm.convergecloud.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.convergecloud.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: luzon
```

3. signing failed

According to the actual situation, there are the following signature failure error codes, please handle according to the actual situation

error code	error description
AuthFailure.SignatureExpire	signature expiration
AuthFailure.SecretIdNotFound	key is not present
AuthFailure.SignatureFailure	signature error
AuthFailure.TokenFailure	token error
AuthFailure.InvalidSecretId	Illegal key (not cloud API key type)

4. Signature Demo

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
```

```
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class CloudAPITC3Demo {
    private final static String CHARSET = "UTF-8";
    private final static String ENDPOINT = "cvm.convergecloud.com";
    private final static String PATH = "/";
    private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
    private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
    private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencode
d";
    private final static String CT_JSON = "application/json";
    private final static String CT_FORM_DATA = "multipart/form-data";

    public static byte[] sign256(byte[] key, String msg) throws Exception {
        Mac mac = Mac.getInstance("HmacSHA256");
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
        mac.init(secretKeySpec);
        return mac.doFinal(msg.getBytes(CHARSET));
    }

    public static void main(String[] args) throws Exception {
        String service = "cvm";
        String host = "cvm.convergecloud.com";
        String region = "luzon";
        String action = "DescribeInstances";
        String version = "2017-03-12";
        String algorithm = "TC3-HMAC-SHA256";
        String timestamp = "1539084154";
        //String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
        SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
        // Pay attention to the time zone, otherwise it is easy to make mistakes.
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ************* Step 1: Assemble the specification request string *************
```

```
        String httpRequestMethod = "GET";
        String canonicalUri = "/";
        String canonicalQueryString = "Limit=10&Offset=0";
        String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host
+ "\n";
        String signedHeaders = "content-type;host";
        String hashedRequestPayload = DigestUtils.sha256Hex("");
        String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryStri
ng + "\n"
                + canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
        System.out.println(canonicalRequest);

        // ************* Step 2: Stitching the string to be signed *************
        String credentialScope = date + "/" + service + "/" + "tc3_request";
        String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
        String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCan
onicalRequest;
        System.out.println(stringToSign);

        // ************* Step 3: Calculate the signature *************
        byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
        byte[] secretService = sign256(secretDate, service);
        byte[] secretSigning = sign256(secretService, "tc3_request");
        String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLow
erCase();
        System.out.println(signature);

        // ************* Step 4: Splicing Authorization *************
        String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
                + "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
        System.out.println(authorization);

        TreeMap<String, String> headers = new TreeMap<String, String>();
        headers.put("Authorization", authorization);
        headers.put("Host", host);
        headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
        headers.put("X-TC-Action", action);
        headers.put("X-TC-Timestamp", timestamp);
        headers.put("X-TC-Version", version);
        headers.put("X-TC-Region", region);
    }
}
```

Python

```
# -*- coding: utf-8 -*-
```

```
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# key parameters
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.convergecloud.com"
endpoint = "https://" + host
region = "luzon"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ************* Step 1: Assemble the specification request string *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
payload = ""
if http_request_method == "POST":
    canonical_querystring = ""
    ct = "json"
    payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
                     canonical_uri + "\n" +
                     canonical_querystring + "\n" +
                     canonical_headers + "\n" +
                     signed_headers + "\n" +
                     hashed_request_payload)
print(canonical_request)

# ************* Step 2: Stitching the string to be signed *************
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
                  str(timestamp) + "\n" +
                  credential_scope + "\n" +
                  hashed_canonical_request)
print(string_to_sign)
```

```
# ************* Step 3: Calculate the signature *************
# Compute signature digest function
def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* Step 4: Splicing Authorization *************
authorization = (algorithm + " " +
                 "Credential=" + secret_id + "/" + credential_scope + ", " +
                 "SignedHeaders=" + signed_headers + ", " +
                 "Signature=" + signature)
print(authorization)

# Common parameters added to request header
headers = {
    "Authorization": authorization,
    "Host": host,
    "Content-Type": "application/%s" % ct,
    "X-TC-Action": action,
    "X-TC-Timestamp": str(timestamp),
    "X-TC-Version": version,
    "X-TC-Region": region,
}
```

request

1. Service Address

Region refers to the geographical area of a physical data center. Converge Cloud ensures complete isolation between different regions, providing maximum stability and fault tolerance. To reduce access latency and improve download speed, it is recommended to choose the region closest to your customers.

You can view the complete region list by using the API interface "DescribeRegions".

2. Communications Protocol

All the Converge Cloud APIs communicate via HTTPS, providing highly secure communication tunnels.

3. Request Methods

Supported HTTP request methods:

- POST (recommended)
- GET

PThe Content-Type types supported by POST requests:

- application/json (recommended). The TC3-HMAC-SHA256 signature algorithm must be used.
- application/x-www-form-urlencoded. The HmacSHA1 or HmacSHA256 signature algorithm must be used.
- multipart/form-data (only supported by certain APIs). You must use TC3-HMAC-SHA256 to calculate the signature.

The size of a GET request packet is up to 32 KB. The size of a POST request is up to 1 MB when the HmacSHA1 or HmacSHA256 signature algorithm is used, and up to 10 MB when TC3-HMAC-SHA256 is used.

4. Character Encoding

Only UTF-8 encoding is used.

result

Response for Successful Requests

For example, when calling CAM API (version: 2017-03-12) to view the status of instances (DescribeInstancesStatus), if the request has succeeded, you may see the response as shown below:


```
{
    "Response": {
        "TotalCount": 0,
        "InstanceStatusSet": [],
        "RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
    }
}
```


- The API will return Response, which contains RequestId, as long as it processes the request. It does not matter if the request is successful or not.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.
- Except for the fixed fields, all fields are action-specified. For the definitions of action-specified fields, see the corresponding API documentation. In this example, TotalCount and InstanceStatusSet are the fields specified by the API DescribeInstancesStatus. 0 TotalCount means that the requester owns 0 CVM instance so the InstanceStatusSet is empty.

Response for Failed Requests

If the request has failed, you may see the response as shown below:


```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```


- The presence of the Error field indicates that the request has failed. A response for a failed request will include Error, Code and Message fields.

- Code is the code of the error that helps you identify the cause and solution. There are two types of error codes so you may find the code in either common error codes or API-specified error codes.
- Message explains the cause of the error. Note that the returned messages are subject to service updates. The information the messages provide may not be up-to-date and should not be the only source of reference.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.

Common Error Codes

If there is an Error field in the response, it means that the API call failed. The Code field in Error indicates the error code. The following table lists the common error codes that all actions can return.

Error Code	Description
AuthFailure.InvalidSecretId	Invalid key (not a API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	The key does not exist.
AuthFailure.SignatureExpire	Signature expired.
AuthFailure.SignatureFailure	Signature error.
AuthFailure.TokenFailure	Token error.
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.

Error Code	Description
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	hHTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

PublicParameter

Common parameters are parameters used to identify users and interface authentication purposes. If not necessary, these parameters are not described in the separate interface document of each interface, but these parameters need to be carried in each request before the request can be normally initiated.

signature method v3

When using TC3-HMAC-SHA256 signature method, the common parameters need to be uniformly placed in the HTTP Header request header, as follows:

parameter name	type	required	described
X-TC-Action	String	Yes	The name of the operation interface. Refer to the description of the public parameter Action in the input parameters of the interface documentation for the value. For example, the value for the query instance list interface of the cloud server is DescribeInstances.
X-TC-Region	String	Yes	region parameters, Data used to identify which region you wish to operate on. The region value accepted by the interface refers to the description of the input parameter common parameter Region in the interface document. Note: Some interfaces do not need to pass this parameter, which is specifically stated in the interface documentation. In this case, even passing this parameter will not take effect.
X-TC-Timestamp	Integer	Yes	The current UNIX timestamp, which records the time when the API request was initiated. for example 1529223702. Note: If the time difference from the server exceeds 5 minutes, it will cause a signature expiration error.
X-TC-Version	String	Yes	Version of API for operation. Refer to the description of the public parameter Version in the interface document for the value. For example, the version of the cloud server. 2017-03-12.
Authorization	String	Yes	HTTP The standard authentication header field is "Authorization". For example: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 Here, - TC3-HMAC-SHA256: Signature method, currently fixed as this value, - Credential: Credential: Signature credential; AKIDEXAMPLE is the SecretId; Date is a date in UTC time, and this value must match the value of X-TC-Timestamp (a common parameter) in UTC time format; service is the name of the product/service, and is generally a domain name prefix. For example,cvm; - SignedHeaders: The headers that contains the authentication information; content-type and host are the required headers; - Signature: Signature digest.
X-TC-Token	String	No	The token used for temporary certificates needs to be used in conjunction with a temporary key. Temporary keys and tokens need to be obtained by calling the access management service interface. Long-term keys do not require tokens.

signature method v1

When using HmacSHA1 and HmacSHA256 signature methods, common parameters need to be placed uniformly in the request string, as follows

parameter name	type	required	described
Action	String	Yes	The name of the interface to be operated. The value refers to the explanation of the public parameter Action in the interface documentation. For example, for the cloud server's query instance list interface, the value is DescribeInstances .
Region	String	Yes	The region parameter is used to identify which region's data you want to operate on. The region value accepted by the interface is specified in the input parameter of the public parameter Region in the interface documentation. Note: Some interfaces do not require this parameter to be passed, which will be specifically mentioned in the interface documentation. Even if this parameter is passed, it will not take effect in this case.
Timestamp	Integer	Yes	The current UNIX timestamp, which can record the time when the API request is initiated. For example, 1529223702. If the difference between the current time is too large, it will cause a signature expiration error.
Nonce	Integer	Yes	A random positive integer combined with Timestamp is used to prevent replay attacks.
SecretId	String	Yes	The SecretId is an identifier applied for the cloud API key to identify the user's identity. A SecretId corresponds to a unique SecretKey , and the SecretKey is used to generate the request signature Signature .
Signature	String	Yes	Request signature is used to verify the legitimacy of this request. Users need to calculate it based on the actual input parameters. The specific calculation method can be found in the interface authentication documentation.
Version	String	Yes	The version of the API being operated on. The value refers to the description of the public parameter Version in the interface documentation. For example, the version of the cloud server. 2017-03-12.
SignatureMethod	String	No	Signature method, currently supports HmacSHA256 and HmacSHA1. HmacSHA256 algorithm is used to verify signatures only if this parameter is specified as HmacSHA 256, otherwise HmacSHA1 is used to verify signatures.
Token	String	No	Token used for temporary certificate needs to be used together with temporary key. The temporary key and Token need to be obtained from the Access Management service invocation interface. Long-term keys do not require tokens.

zone list

A region (Region) refers to the geographical area of a physical data center. Converge Cloud Translation: To deliver verification that completely isolates different regions, ensuring maximum stability and fault tolerance between regions. In order to reduce access latency and improve download speed, it is recommended that you choose the region closest to your customers.

You can view the complete region list by using the API interface Query Region List.

Department and Member Management APIs
AddOrganizationMemberEmail

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to add organization members' email addresses.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AddOrganizationMemberEmail
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberUin	Yes	Yes	Int64	Member UIN. Example: 111111111111
Email	Yes	Yes	String	Email address. Example: 12***@XX.com
CountryCode	Yes	Yes	String	International area code. Example: 86

Parameter name	Required	Allow NULL	Type	Description
Phone	Yes	Yes	String	Phone number. Example: 18***11

3. Output Parameters

Parameter name	Type	Description
BindId	Uint64	Bound ID. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
UnsupportedOperation	
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.
FailedOperation.CheckMailAccount	
FailedOperation.CheckAccountPhoneBindLimit	
LimitExceeded.PhoneNumBound	
FailedOperation.MemberEmailExist	
LimitExceeded.EmailBindOverLimit	

Error Code	Description
FailedOperation.EmailAlreadyUsed	

CheckAccountDelete

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to check whether a member account can be deleted.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CheckAccountDelete
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberUin	Yes	Yes	Int64	Member UIN. Example: 111111111111

3. Output Parameters

Parameter name	Type	Description
AllowDelete	Bool	Specifies whether a member can be deleted. true: yes; false: no. Example: true
NotAllowReason	NotAllowReason	Reasons for not allowing deletion. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
ResourceNotFound.MemberNotExist	
InvalidParameter	
InternalError	
UnsupportedOperation	

CreateOrganizationMember

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to create an organization member.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateOrganizationMember
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IdentityRoleID	No	Yes	Array of Uint64	List of member access identity IDs, which can be obtained by calling ListOrganizationIdentity. Example: [1]
Name	Yes	Yes	String	Member name, which contains up to 25 characters, including English letters, digits, and symbols +@&_[]-:, . Example: member_name
PermissionIds	Yes	Yes	Array of Uint64	List of member financial permission IDs. Valid values: 1: View bills. 2: View balance. 3: Transfer funds. 4: Consolidate bills. 5: Issue invoice. 6: Inherit discounts. 7: Pay on behalf. 1 and 2 are required by default. Example: [1,2]
AccountName	Yes	Yes	String	Account name. The maximum length is 25 characters. Supported characters include English letters, digits, and symbols +@&_[]-:, Example: member_name
Remark	No	Yes	String	Remarks. Example: create member
RecordId	No	Yes	Int64	Member creation record ID, which is required when creation fails and needs to be retried. Example: 0
PayUin	No	Yes	String	Payer UIN, which is required when pay-on-behalf mode is used. Example: 100000000001
AuthRelationId	No	Yes	Int64	Verified entity relationship ID, which is mandatory for creating members for different entities. The value can be obtained by calling DescribeOrganizationAuthNode. Example: 0
PolicyType	Yes	Yes	String	Relationship policy. Valid value: Financial . Example: Financial
NodeId	Yes	Yes	Int64	Node ID of the member's department. It can be obtained through DescribeOrganizationNodes. Example: 1001

3. Output Parameters

Parameter name	Type	Description
Uin	Int64	Member UIN. Example: 111111111111
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
FailedOperation.MemberNameUsed	
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.
FailedOperation.AuthInfoEmpty	
FailedOperation.AuthNotEnterprise	
FailedOperation.OrganizationNodeNotExist	
FailedOperation.OrganizationPolicyIllegal	
FailedOperation.OrganizationPermissionIllegal	
LimitExceeded.OrganizationMemberOverLimit	
FailedOperation.OrganizationMemberNameUsed	
ResourceNotFound.OrganizationNodeNotExist	The organization node does not exist.
LimitExceeded.CreateMemberOverLimit	
FailedOperation.CreateAccount	
FailedOperation.CreateRole	
FailedOperation.CreateRecordNotExist	
FailedOperation.CreateRecordAlreadySuccess	
FailedOperation.CreateMemberAuthOverLimit	
FailedOperation.PayUinIllegal	
FailedOperation.OperateBillingPermissionErr	
UnsupportedOperation.AddDelegatePayerNotAllow	

Error Code	Description
UnsupportedOperation.AddDiscountInheritNotAllow	
UnsupportedOperation.MemberDiscountInheritExisted	
UnsupportedOperation.OwnerDiscountInheritExisted	
UnsupportedOperation.PayerArrearsAndNoCreditAccount	
UnsupportedOperation.OrderInProgressExisted	
UnsupportedOperation.MemberAccountArrears	
UnsupportedOperation.MemberIsAgent	
UnsupportedOperation.ManagementSystemError	
UnsupportedOperation.InconsistentUserTypes	
UnsupportedOperation.PayerExistAccountLevelDiscountInherit	
UnsupportedOperation.MemberExistAccountLevelDiscountInherit	
ResourceNotFound.OrganizationAuthRelationNotExist	
FailedOperation.GetAuthInfo	
InvalidParameter.OrganizationMemberNotExist	
UnsupportedOperation.ExistedAgent	
UnsupportedOperation.ExistedClient	
FailedOperation.CreateBillingPermissionErr	
FailedOperation.PartnerManagementErr	
UnsupportedOperation.AbnormalFinancialStatusOfAdmin	
UnsupportedOperation.SecondaryDistributorSubClientExisted	

DeleteAccount

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

Delete the member account.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteAccount
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberUin	Yes	Yes	Int64	Member UIN. Example: 111111111111

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
ResourceNotFound.MemberNotExist	
InvalidParameter	
InternalError	
UnsupportedOperation.MemberExistServiceNotAllowDelete	
FailedOperation.OrganizationAuthManageNotAllowDelete	
FailedOperation.MemberShareResource	
UnsupportedOperation.InviteAccountNotAllowDelete	
UnsupportedOperation.DeleteAccountDisabled	
UnsupportedOperation.MemberAccountExistResource	
UnsupportedOperation	

DeleteOrganizationMembers

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to remove a member account from the organization, rather than delete the account.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteOrganizationMembers
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberUin	Yes	Yes	Array of Int64	Uin list of the deleted members. Example: [111111111111]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.DisableQuitSelfCreatedOrganization	
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	
FailedOperation.QuitShareUintError	
UnsupportedOperation.CreateMemberNotAllowDelete	
FailedOperation.MemberExistDelegatePayerNotAllowDelete	
FailedOperation.MemberIsDelegatePayerNotAllowDelete	
FailedOperation.OperateBillingPermissionErr	
UnsupportedOperation.MemberExistServiceNotAllowDelete	
FailedOperation.OrganizationAuthManageNotAllowDelete	
FailedOperation.ShareResourceMemberInUse	
FailedOperation.MemberShareResource	
UnsupportedOperation.MemberExistOperateProcessNotAllowDelete	
UnsupportedOperation.MemberNoPayment	

DescribeOrganizationMemberEmailBind

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to query the detailed information of a member's email binding.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeOrganizationMemberEmailBind
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberUin	Yes	Yes	Int64	Member UIN. Example: 111111111111

3. Output Parameters

Parameter name	Type	Description
ApplyTime	String	Application time. Example: 2022-01-13 12:08:09
Email	String	Email address. Example: 12***@XX.com
BindTime	String	Binding time. Example: 2022-01-13 18:08:09
CountryCode	String	International area code. Example: 86

Parameter name	Type	Description
PhoneBind	Uint64	Security phone number binding status. 0: not bound; 1: bound. Example: 0
BindId	Uint64	Bound ID. Example: 12
Phone	String	Security phone number. Example: 18***32
BindStatus	String	Binding status. Unbound: not bound; valid: pending activation; success: bound; failed: failed. Example: Success
Description	String	Failure description. Example: success
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.UserNotExist	
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.
FailedOperation.EmailAlreadyUsed	
FailedOperation.BindEmailLinkInvalid	
FailedOperation.BindEmailLinkExpired	
FailedOperation.MemberBindPhoneError	
FailedOperation.EmailBindRecordInvalid	
FailedOperation.MemberBindEmailError	
FailedOperation.AccountAlreadyRegister	
InvalidParameter.PasswordIllegal	
InvalidParameter.InvalidEmail	
InvalidParameter.CodeExpired	

Error Code	Description
InvalidParameter.CodeError	

SendOrgMemberAccountBindEmail

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to resend the activation email for binding a member's email address.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: SendOrgMemberAccountBindEmail
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberUin	Yes	Yes	Int64	Member UIN. Example: 111111111111
BindId	Yes	Yes	Int64	Binding ID. It can be obtained through DescribeOrganizationMemberEmailBind. Example: 12

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.

Error Code	Description
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.
ResourceNotFound.EmailBindRecordNotExist	
FailedOperation.EmailBindRecordInvalid	
LimitExceeded.SendEmailLimit	
LimitExceeded.SendEmailWithinOneHourLimit	

UpdateOrganizationMember

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to update organization member information.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateOrganizationMember
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IsAllowQuit	No	Yes	String	Whether to allow members to exit an organization. Valid values: Allow: permitted, Denied: not permitted. Example: allow
PayUin	No	Yes	String	Payer UIN, which is required when pay-on-behalf mode is used in member financial permission. The value is the principal administrator UIN of the corresponding member. Example: 100000000001
MemberUin	Yes	Yes	Uint64	Member UIN. Example: 111111111111
Name	No	Yes	String	Member name, which contains up to 25 characters, including English letters, digits, and symbols +@&_[]-, . Example: member_name
Remark	No	Yes	String	Remarks, which contain up to 40 characters. Example: create member
PolicyType	No	Yes	String	Relationship policy type. When PolicyType is not empty, PermissionIds cannot be empty. Value: Financial. Example: Financial
PermissionIds	No	Yes	Array of Uint64	List of member financial permission IDs. When PermissionIds is not empty, PolicyType cannot be empty. Valid values: 1: bill viewing; 2: balance viewing; 3: fund transfer; 4: consolidated billing; 5: invoicing; 6: discount inheritance; 7: proxy payment; 8: cost analysis. If this parameter is not empty, permissions 1 and 2 are mandatory by default. Example: [1,2]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
FailedOperation.MemberNameUsed	
ResourceNotFound.MemberNotExist	
UnsupportedOperation	
FailedOperation.AuthInfoEmpty	
FailedOperation.AuthNotEnterprise	
FailedOperation.OrganizationPolicyIllegal	
FailedOperation.OrganizationPermissionIllegal	
FailedOperation.OrganizationMemberNameUsed	
FailedOperation.AuthInfoNotSame	
FailedOperation.ChangePermissionRecordExist	
FailedOperation.PayUinIllegal	
FailedOperation.OperateBillingPermissionErr	
UnsupportedOperation.DeleteDelegatePayerNotAllow	
UnsupportedOperation.AddDelegatePayerNotAllow	
UnsupportedOperation.MemberNotAllowQuit	
UnsupportedOperation.AddDiscountInheritNotAllow	
UnsupportedOperation.MemberDiscountInheritExisted	
UnsupportedOperation.OwnerDiscountInheritExisted	
UnsupportedOperation.PayerArrearsAndNoCreditAccount	
UnsupportedOperation.OrderInProgressExisted	
UnsupportedOperation.MemberAccountArrears	
UnsupportedOperation.MemberIsAgent	
UnsupportedOperation.ManagementSystemError	
UnsupportedOperation.InconsistentUserTypes	
UnsupportedOperation.PayerExistAccountLevelDiscountInherit	
UnsupportedOperation.MemberExistAccountLevelDiscountInherit	
InvalidParameter.AllowQuitIllegal	
UnsupportedOperation.ExistedAgent	
UnsupportedOperation.ExistedClient	
FailedOperation.CreateBillingPermissionErr	

UpdateOrganizationMemberEmailBind

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to modify the email address bound to a member.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateOrganizationMemberEmailBind
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Phone	Yes	Yes	String	Phone number. Example: 18***32
MemberUin	Yes	Yes	Int64	Member UIN. Example: 111111111111
BindId	Yes	Yes	Int64	Binding ID. It can be obtained through DescribeOrganizationMemberEmailBind. Example: 12
Email	Yes	Yes	String	Email address. Example: 12***@XX.com
CountryCode	Yes	Yes	String	International area code. Example: 86

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
UnsupportedOperation	
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.
FailedOperation.CheckMailAccount	
FailedOperation.EmailAlreadyUsed	
ResourceNotFound.EmailBindRecordNotExist	
FailedOperation.EmailBindRecordInvalid	
LimitExceeded.UpdateEmailBindOverLimit	

Financial Overview APIs DescribeOrganizationFinancialByMember

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to obtain organizational financial information by member dimension.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeOrganizationFinancialByMember
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ProductCodes	No	Yes	Array of String	Query the product list. A maximum of 100 products can be queried. Example: ["p_cvm"]
Month	Yes	Yes	String	Start month of query. The format should be yyyy-mm, for example, 2021-01. Example: 2021-01
Limit	No	Yes	Int64	Limit. Value range: 1-50. Default value: 10. Example: 5
Offset	No	Yes	Int64	Offset. Its value must be an integer multiple of the limit. Default value: 0. Example: 0
EndMonth	No	Yes	String	End month of query. The format should be yyyy-mm, for example, 2021-01. The default value is the start month of query. Example: 2021-05
MemberUins	No	Yes	Array of Int64	Queried member list. A maximum of 100 members can be queried. Example: [100000000001]

3. Output Parameters

Parameter name	Type	Description
TotalCost	Float	Total consumption of the current month. Example: 10.01
Items	Array of OrgMemberFinancial	Member consumption details. Example:View
Total	Int64	Total count. Example: 2
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	
InternalError	

DescribeOrganizationFinancialByMonth

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to obtain the monthly trend of organizational financial information.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeOrganizationFinancialByMonth
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Limit	No	Yes	Int64	Number of months for query. Value range: 1–6; default value: 6. Example: 5
EndMonth	No	Yes	String	End month of query. The format should be yyyy-mm, for example, 2021-01. Example: 2023-01
MemberUins	No	Yes	Array of Int64	Queried member list. A maximum of 100 members can be queried. Example: [100000000001]
ProductCodes	No	Yes	Array of String	Query the product list. A maximum of 100 products can be queried. Example: ["p_cvm"]

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
Items	Array of OrgFinancialByMonth	Product consumption details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	
InternalError	

DescribeOrganizationFinancialByProduct

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to obtain organizational financial information by product dimension.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeOrganizationFinancialByProduct
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
EndMonth	No	Yes	String	End month of query. The format should be yyyy-mm, for example, 2021-01. The default value is the start month of query. Example: 2021-01
MemberUins	No	Yes	Array of Int64	Queried member list. A maximum of 100 members can be queried. Example: [100000000001]
ProductCodes	No	Yes	Array of String	Query the product list. A maximum of 100 products can be queried. Example: ["p_cvm"]
Month	Yes	Yes	String	Start month of query. The format should be yyyy-mm, for example, 2021-01. Example: 2021-01
Limit	No	Yes	Int64	Limit. Value range: 1-50. Default value: 10. Example: 5
Offset	No	Yes	Int64	Offset. Its value must be an integer multiple of the limit. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
TotalCost	Float	Total consumption of the current month. Example: 43.35
Items	Array of OrgProductFinancial	Product consumption details. Example:View
Total	Int64	Total count. Example: 2
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	
InternalError	

Organization Management Policy APIs
ListPolicies

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to query and view the policy list data.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ListPolicies
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Rp	No	Yes	Uint64	Items per page, which should be greater than 0 and less than or equal to 200. The default value is 20. Example: 1
Page	No	Yes	Uint64	Page number, which starts from 1 and cannot exceed 200. The default value is 1. Example: 10
Scope	No	Yes	String	Query range. Valid values: All: all policies; QCS; only preset policies; Local: only custom policies. The default value is All. Example: All
Keyword	No	Yes	String	Search keyword. Searches can be performed by policy name. Example: policy_name
PolicyType	No	Yes	String	Policy type. Valid values: SERVICE_CONTROL_POLICY: service control policy; TAG_POLICY: tag policy. The default value is SERVICE_CONTROL_POLICY. Example: SERVICE_CONTROL_POLICY

3. Output Parameters

Parameter name	Type	Description
TotalNum	Uint64	Total policies Example: 1
List	Array of ListPolicyNode	Policy list data. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.InvitationNotExist	
ResourceNotFound.UserNotExist	
ResourceNotFound.OrganizationNotExist	The organization does not exist.
ResourceNotFound.MemberNotExist	
ResourceNotFound.NodeNotExist	
MissingParameter	
InvalidParameter	
InternalError	
ResourceUnavailable	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.
ResourceNotFound.OrganizationNodeNotExist	The organization node does not exist.
ResourceNotFound.ApplyNotExist	

Error Code	Description
ResourceNotFound.ServiceRoleNotExist	
ResourceNotFound.MemberPolicyNotExist	Policy authorization does not exist.
ResourceNotFound.MemberIdentityNotExist	The member role identity does not exist.
ResourceNotFound.ChangePermissionNotExist	
ResourceNotFound.OrganizationIdentityNotExist	
ResourceNotFound.PolicyNotExist	
ResourceNotFound.EmailBindRecordNotExist	
ResourceNotFound.MemberEventNotExist	
ResourceNotFound.MemberOperateProcessNotExist	
ResourceNotFound.ShareResourceMemberNotExist	
ResourceNotFound.OrganizationServiceNotExist	
ResourceNotFound.OrganizationServiceAssignNotExist	
ResourceNotFound.OrganizationAuthRelationNotExist	
ResourceNotFound.ResourceTypeNotExist	
InvalidParameter.InterfaceNotExist	
InvalidParameter.OrganizationNotExist	
InvalidParameter.OrganizationNodeNotExist	
InvalidParameter.OrganizationMemberNotExist	
InvalidParameter.OrganizationMemberNotManager	
ResourceNotFound.NotFound	
ResourceNotFound.PolicyIdNotFound	

ListPoliciesForTarget

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to query the list of policies associated with a target.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ListPoliciesForTarget
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Rp	No	Yes	Uint64	Items per page, which should be greater than 0 and less than or equal to 200. The default value is 20. Example: 1
Page	No	Yes	Uint64	Page number, which starts from 1 and cannot exceed 200. The default value is 1. Example: 10
TargetId	Yes	Yes	Uint64	Account UIN or node ID. Example: 10083
PolicyType	No	Yes	String	Policy type. Valid values: SERVICE_CONTROL_POLICY: service control policy; TAG_POLICY: tag policy. The default value is SERVICE_CONTROL_POLICY. Example: SERVICE_CONTROL_POLICY
Keyword	No	Yes	String	Search keywords. Searches can be performed by policy name. Example: policy_name

3. Output Parameters

Parameter name	Type	Description
TotalNum	Uint64	Total number. Example: 1
List	Array of ListPoliciesForTarget	List of policies associated with a target. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.InvitationNotExist	
ResourceNotFound.UserNotExist	
ResourceNotFound.OrganizationNotExist	The organization does not exist.
ResourceNotFound.MemberNotExist	
ResourceNotFound.NodeNotExist	
MissingParameter	
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.
ResourceNotFound.OrganizationNodeNotExist	The organization node does not exist.
ResourceNotFound.ApplyNotExist	
ResourceNotFound.ServiceRoleNotExist	
ResourceNotFound.MemberPolicyNotExist	Policy authorization does not exist.

Error Code	Description
ResourceNotFound.MemberIdentityNotExist	The member role identity does not exist.
ResourceNotFound.ChangePermissionNotExist	
ResourceNotFound.OrganizationIdentityNotExist	
ResourceNotFound.PolicyNotExist	
ResourceNotFound.EmailBindRecordNotExist	
ResourceNotFound.MemberEventNotExist	
ResourceNotFound.MemberOperateProcessNotExist	
ResourceNotFound.ShareResourceMemberNotExist	
ResourceNotFound.OrganizationServiceNotExist	
ResourceNotFound.OrganizationServiceAssignNotExist	
ResourceNotFound.OrganizationAuthRelationNotExist	
ResourceNotFound.ResourceTypeNotExist	
InvalidParameter.InterfaceNotExist	
InvalidParameter.OrganizationNotExist	
InvalidParameter.OrganizationNodeNotExist	
InvalidParameter.OrganizationMemberNotExist	
InvalidParameter.OrganizationMemberNotManager	
ResourceNotFound.NotFound	
ResourceNotFound.PolicyIdNotFound	

Organization Settings APIs CreateOrganization

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to create an organization.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateOrganization
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
OrgId	Uint64	Organization ID. Example: 101

Parameter name	Type	Description
NickName	String	Creator's nickname. Example: nick_name
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.OrganizationExistAlready	
UnsupportedOperation	
InvalidParameter	
InternalError	
FailedOperation.AuthInfoEmpty	
FailedOperation.AuthNotEnterprise	
UnsupportedOperation.CreateMemberNotAllowCreateOrganization	

DeleteOrganization

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to delete an organization.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteOrganization
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
FailedOperation.OrganizationNotEmpty	
InvalidParameter	
InternalError	
FailedOperation.ShareUnitNotEmpty	
FailedOperation.QuitShareUint	
FailedOperation.QuiteShareUnit	
FailedOperation.MemberExistDelegatePayerNotAllowDelete	
FailedOperation.MemberIsDelegatePayerNotAllowDelete	
FailedOperation.OrganizationPolicyIsNotDisabled	

QuitOrganization

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to exit an organization.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: QuitOrganization
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
OrgId	Yes	Yes	Uint64	Organization ID. Example: 101

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.DisableQuitSelfCreatedOrganization	
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.
FailedOperation.QuiteShareUnit	
UnsupportedOperation.CreateMemberNotAllowQuit	
FailedOperation.MemberExistDelegatePayerNotAllowDelete	
FailedOperation.MemberIsDelegatePayerNotAllowDelete	
FailedOperation.OperateBillingPermissionErr	
UnsupportedOperation.MemberNotAllowQuit	
UnsupportedOperation.MemberExistServiceNotAllowDelete	
FailedOperation.OrganizationAuthManageNotAllowDelete	
FailedOperation.ShareResourceMemberInUse	
FailedOperation.MemberShareResource	
UnsupportedOperation.MemberExistOperateProcessNotAllowDelete	
UnsupportedOperation.MemberNoPayment	

Unified Member Login APIs CreateOrganizationIdentity

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to add an organization identity.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateOrganizationIdentity
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IdentityAliasName	Yes	Yes	String	Identity name Example: admin_identity
Description	No	Yes	String	Identity description. Example: admin identity
IdentityPolicy	Yes	Yes	Array of IdentityPolicy	Identity policy. Example:View

3. Output Parameters

Parameter name	Type	Description
IdentityId	Uint64	Identity ID. Example: 1001
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	
FailedOperation.OrganizationIdentityNameUsed	
ResourceNotFound.PolicyNotExist	
LimitExceeded.IdentityExceedLimit	
FailedOperation.GetPolicyDetail	

CreateOrganizationMemberAuthIdentity

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to add organization member access authorization.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateOrganizationMemberAuthIdentity
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberUins	Yes	Yes	Array of Uint64	Member UIN list, including up to 10 items. Example: [111111111111]
IdentityIds	Yes	Yes	Array of Uint64	List of dentity IDs (up to 5). It can be obtained through ListOrganizationIdentity. Example: [13]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
UnsupportedOperation	
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.
FailedOperation.CreateRole	
ResourceNotFound.OrganizationIdentityNotExist	
FailedOperation.OrganizationIdentityPolicyError	

CreateOrganizationMembersPolicy

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to create an organization member access policy.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateOrganizationMembersPolicy
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberUins	Yes	Yes	Array of Int64	Member UIN list, including up to 10 items. Example: [111111111111]
PolicyName	Yes	Yes	String	Policy name, which contains 1 to 128 characters, including English letters, digits, and symbols +=,.@_-. Example: policy_name
IdentityId	Yes	Yes	Int64	Member access identity ID. It can be obtained through ListOrganizationIdentity. Example: 101
Description	No	Yes	String	Policy description, which contains up to 128 characters. Example: description

3. Output Parameters

Parameter name	Type	Description
PolicyId	Int64	Policy ID. Example: 1001
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
UnsupportedOperation	

Error Code	Description
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.
ResourceNotFound.MemberIdentityNotExist	The member role identity does not exist.
FailedOperation.MemberPolicyNameExist	
FailedOperation.CreatePolicy	

DeleteOrganizationIdentity

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to delete an organization identity.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteOrganizationIdentity
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IdentityId	Yes	Yes	Uint64	Identity ID. It can be obtained through ListOrganizationIdentity. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationIdentityNotExist	
FailedOperation.OrganizationIdentityInUsed	

DeleteOrganizationMemberAuthIdentity

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to delete organization member access authorization.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteOrganizationMemberAuthIdentity
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberUin	Yes	Yes	Uint64	Member UIN. Example: 111111111111
IdentityId	Yes	Yes	Uint64	Identity ID. It can be obtained through ListOrganizationIdentity. Example: 11

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	
ResourceNotFound.MemberIdentityNotExist	The member role identity does not exist.
ResourceNotFound.OrganizationIdentityNotExist	
FailedOperation.MemberIdentityAuthUsed	

DeleteOrganizationMembersPolicy

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to delete an organization member access policy.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteOrganizationMembersPolicy
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
PolicyId	Yes	Yes	Uint64	Access policy ID. It can be obtained through DescribeOrganizationMemberPolicies. Example: 1001

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	
ResourceNotFound.MemberPolicyNotExist	Policy authorization does not exist.

Error Code	Description
FailedOperation.DeletePolicy	

DescribeOrganizationMemberAuthIdentities

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to obtain the list of organization member access authorization.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeOrganizationMemberAuthIdentities
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberUin	No	Yes	Int64	Uin of the organization member. At least one of the input parameters MemberUin and IdentityId must be entered. Example: 11111111111
IdentityId	No	Yes	Uint64	Identity ID. Either MemberUin and IdentityId must be filled in. It can be obtained through ListOrganizationIdentity. Example: 1
Offset	Yes	Yes	Int64	Offset. Its value must be an integer multiple of the limit. Default value: 0. Example: 0
Limit	Yes	Yes	Int64	Limit. Value range: 1-50. Default value: 10. Example: 10

3. Output Parameters

Parameter name	Type	Description
Items	Array of OrgMemberAuthIdentity	List of authorized identities. Example:View
Total	Uint64	Total count. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	

DescribeOrganizationMemberPolicies

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to get the list of organization member authorization policies.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeOrganizationMemberPolicies
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
SearchKey	No	Yes	String	Search keyword, which can be the policy name or description. Example: policy_name
Offset	Yes	Yes	Int64	Offset. Its value must be an integer multiple of the limit. Default value: 0. Example: 0
Limit	Yes	Yes	Int64	Limit. Value range: 1-50. Default value: 10. Example: 10
MemberUin	Yes	Yes	Int64	Member UIN. Example: 111111111111

3. Output Parameters

Parameter name	Type	Description
Total	Uint64	Total count. Example: 1

Parameter name	Type	Description
Items	Array of OrgMemberPolicy	Member access policy list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.

ListOrganizationIdentity

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to obtain the list of organization member access identities.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ListOrganizationIdentity
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Limit	Yes	Yes	Uint64	Limit. Value range: 1-50. Default value: 10. Example: 10
SearchKey	No	Yes	String	Keyword for search by name. Example: identity_name
IdentityId	No	Yes	Uint64	Identity ID, which can be searched by identity ID. Example: 1
IdentityType	No	Yes	Uint64	Identity type. Valid values: 1: preset; 2: custom. Example: 1
Offset	Yes	Yes	Uint64	Offset. Its value must be an integer multiple of the limit. Default value: 0. Example: 1

3. Output Parameters

Parameter name	Type	Description
Total	Int64	Total number. Example: 1

Parameter name	Type	Description
Items	Array of OrgIdentity	Item details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	

UpdateOrganizationIdentity

1. Interface Description

Interface request domain name: organization.api3.convergecloud.com.

This API is used to update an organization identity.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-09 21:54:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateOrganizationIdentity
Version	Yes	No	String	Public parameter, The value of this interface: 2022-05-08
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Description	Yes	Yes	String	Identity description. Example: admin identity
IdentityPolicy	Yes	Yes	Array of IdentityPolicy	Identity policy. Example:View
IdentityId	Yes	Yes	Uint64	Identity ID. It can be obtained through ListOrganizationIdentity. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.OrganizationNotExist	The organization does not exist.
InvalidParameter	
InternalError	
ResourceNotFound.OrganizationIdentityNotExist	
ResourceNotFound.PolicyNotExist	
FailedOperation.GetPolicyDetail	

Data structure

Identity

Authorization Identity

Referenced by the following interfaces: DescribeOrganizationMember, DescribeOrganizationMembers

name	required	NULL allowed	type	description
IdentityId	yes	no	Uint64	ID Example: 1
IdentityAliasName	no	no	String	Alias Example: my_identity

AddOrgMember

Referenced by the following interfaces: CreateOrganizationMembers

name	required	NULL allowed	type	description
Remark	no	yes	String	Description Example: ""
MemberUin	yes	yes	Int64	Member UIN. Example: 1000001
MemberName	yes	yes	String	Member name Example: tt
PolicyType	yes	yes	String	Relationship policy type. Example: Finical
PermissionIds	yes	yes	Array of Int64	Relational policy permission ID list. Example: 1
NodeId	yes	yes	Int64	Node ID. Example: 1002

FinancialProductInfo

Referenced by the following interfaces: ListFinancialProduct

name	required	NULL allowed	type	description
ProductCode	yes	yes	String	Product abbreviation. Example: p_gme
ProductName	yes	yes	String	Product name. Example: Game Multimedia Engine

IdentityPolicy

Referenced by the following interfaces: CreateOrganizationIdentity, DescribeOrganizationIdentity, ListOrganizationIdentity, UpdateOrganizationIdentity

name	required	NULL allowed	type	description
PolicyDocument	no	yes	String	Custom policy content, which follows the CAM policy syntax. It is valid and mandatory when PolicyType is a custom policy. Example: { "version": "2.0", "statement": [{ "effect": "allow", "action": ["vpc:*], *"resource": [""] }] }
PolicyId	yes	no	Uint64	CAM preset policy ID, which is valid and required when PolicyType is a preset policy. Example: 1
PolicyName	yes	no	String	CAM preset policy name, which is valid and required when PolicyType is a preset policy. Example: AdministratorAccess
PolicyType	no	yes	Uint64	Policy type. Valid values: 1: custom policy; 2: preset policy. The default value is 2. Example: 2

OrgNodeMemberRecord

Referenced by the following interfaces: DescribeOrganizationNodeMemberRecords

name	required	NULL allowed	type	description
BeforeNodeId	yes	yes	Int64	Node ID before moving. Example: 1
BeforeNodeName	yes	yes	String	Node name before moving. Example: node_name
CurrentNodeName	yes	yes	String	Current node name. Example: node_name
CreateTime	yes	yes	String	Creation time. Example: 2021-02-12 12:12:10
UpdateTime	yes	yes	String	Update time. Example: 2021-02-12 12:12:10
Id	yes	no	Int64	Record ID. Example: 1
OrgId	yes	yes	Int64	Organization ID. Example: 10
MemberUin	yes	yes	Int64	Member UIN. Example: 1000001

name	required	NULL allowed	type	description
MemberName	yes	yes	String	Member name. Example: member_name
CurrentNodeId	yes	yes	Int64	Current node ID. Example: 2

OrgMember

Member account

Referenced by the following interfaces: DescribeOrganizationMembers

name	required	NULL allowed	type	description
MemberUin	no	no	Uint64	Member Account UIN Example: 1000001
Name	no	no	String	Name Example: member_name
MemberType	no	no	String	Member Type Example: Invite
OrgPolicyType	no	no	String	Group Policy Type Example: Financial
OrgPolicyName	no	no	String	Group Policy Name Example: Financial management
OrgPermission	no	no	Array of Permission	Group Permissions Example:View
PayUin	no	no	String	Pay-on-Behalf UIN Example: "100000000001"
PayName	no	no	String	Pay-on-Behalf Username Example: "host_member"
NodeId	no	no	Uint64	Node ID Example: 1002
NodeName	no	no	String	Server name Example: Root
Remark	no	no	String	Remarks Example: member1
IsAllowQuit	no	no	String	Quitting allowed Example: Allow
PermissionStatus	no	no	String	Permission status Example: Confirmed
OrgIdentity	no	no	Array of Identity	Authorization Identity List Example:View
CreateTime	no	no	String	Creation Time Example: 2021-03-12 12:12:22
UpdateTime	no	no	String	Update time Example: 2021-03-12 12:12:22
IsManager	no	no	Int64	Is it an administrator? Example: 1
BindStatus	no	yes	String	Security information binding status. Unbound: not bound; Valid: pending activation; Success: bound; Failed: failed. Example: Unbound
AuthName	no	yes	String	Verified Name Example: auth_name
AuthStatus	no	yes	Uint64	Member entity status. 1: normal; 2: administration to be changed to a member; 3: administrator changed, pending account trust re-establishment; 4: member changed, pending account trust re-establishment; 5: member changed, pending entity association. Example: 1
Tags	no	no	Array of Tags	Member tag list. Example:View

OrgMemberPolicy

Referenced by the following interfaces: DescribeOrganizationMemberPolicies, DescribeOrganizationMembersAuthAccount

name	required	NULL allowed	type	description
PolicyId	yes	yes	Int64	Policy ID. Example: 1001
PolicyName	yes	yes	String	Policy name. Example: policy_name
IdentityId	yes	yes	Int64	Identity ID. Example: 1
IdentityRoleName	yes	yes	String	Identity role name. Example: identity_role
IdentityRoleAliasName	yes	yes	String	Role alias of an identity. Example: identity_name
Description	yes	yes	String	Description. Example: admin identity
CreateTime	yes	yes	String	Creation time. Example: 2021-02-12 12:12:10

name	required	NULL allowed	type	description
UpdateTime	yes	yes	String	Update time. Example: 2021-02-12 12:12:10

Permission

Organization Policy Permissions

Referenced by the following interfaces: DescribeOrganization, DescribeOrganizationMember, DescribeOrganizationMembers, DescribeOrganizationNodeMembers

name	required	NULL allowed	type	description
Id	no	no	Uint64	ID Example: 1
Name	no	no	String	Name Example: View Bills

OrgProductFinancial

Referenced by the following interfaces: DescribeOrganizationFinancialByProduct

name	required	NULL allowed	type	description
ProductName	yes	yes	String	Product code. Example: p_cos
ProductCode	yes	yes	String	Product name. Example: Cloud Object Storage (COS)
TotalCost	yes	yes	Float	Product consumption. Example: 23.22
Ratio	yes	yes	String	Percentage. Example: 34

OrgNodeRecord

Referenced by the following interfaces: DescribeOrganizationNodeRecords

name	required	NULL allowed	type	description
BeforeNodeName	yes	yes	String	Previous node name. The value is empty if the node does not exist. Example: node_name
CurrentNodeName	yes	yes	String	Current node name. The value is empty if the node does not exist. Example: node_name
UpdateTime	yes	yes	String	Update time Example: 2021-02-12 12:12:10
RecordAction	yes	yes	String	Node operation. Create: creation; Delete: deletion; Move: moving. Example: Create
BeforeNodeId	yes	yes	Int64	Previous node ID. The value is 0 if the node does not exist. Example: 11
CurrentNodeId	yes	yes	Int64	Current node ID. The value is 0 if the node does not exist. Example: 12
CreateTime	yes	yes	String	Creation Time Example: 2021-02-12 12:12:10
Id	yes	no	Int64	Record ID Example: 1
OrgId	yes	yes	Int64	Organization ID Example: 11
NodeId	yes	yes	Int64	Node ID Example: 12
NodeName	yes	yes	String	Node name Example: node_name

ListPolicyNode

Referenced by the following interfaces: ListPolicies

name	required	NULL allowed	type	description
PolicyId	yes	no	Uint64	Policy ID Example: 1001
UpdateTime	yes	yes	String	Policy Update Time Example: 2022-08-02 19:40:09
Type	yes	no	Uint64	Policy type. 1: custom; 2: preset. Example: 1
AddTime	yes	yes	String	Policy creation time Example: 2022-08-02 19:40:09
AttachedTimes	yes	yes	Uint64	Policy binding count. Example: 3
Description	yes	yes	String	Policy description information. Example: Policy 1
PolicyName	yes	no	String	Policy Name Example: name_bind

OrgNode

Organization Node

Referenced by the following interfaces: DescribeAllParentNodes, DescribeOrganizationMemberNodes, DescribeOrganizationNodeByName, DescribeOrganizationNodes, DescribeOrganizationNodesByParent

name	required	NULL allowed	type	description
NodeId	no	no	Int64	Node ID Example: 1001
ParentNodeId	no	no	Int64	Parent node ID Example: 1000
Name	no	no	String	Name Example: node_name
Remark	no	no	String	Remarks Example: root node
CreateTime	no	no	String	Creation Time Example: 2021-03-12 12:12:11
UpdateTime	no	no	String	Update time Example: 2021-03-12 12:12:11
Tags	no	no	Array of Tags	Tag Example:View

OrgSubAccountByDay

Referenced by the following interfaces: DescribeOrganizationSubAccountByDay

name	required	NULL allowed	type	description
Id	yes	yes	Int64	Record ID. Example: 1
Day	yes	yes	String	Date in the format of yyyy-mm-dd. For example: 2021-06-09. Example: 2021-06-09
SubAccountNum	yes	yes	Int64	Total number of sub-accounts on the current day. Example: 11
MemberNum	yes	yes	Int64	Total number of members on the current day. Example: 10

AuthRelationFile

Referenced by the following interfaces: InviteOrganizationMember

name	required	NULL allowed	type	description
Name	no	yes	String	File name. Example: file_name
Url	no	yes	String	File path. Example: file/file_name.txt

OrgFinancialByMonth

Referenced by the following interfaces: DescribeOrganizationFinancialByMonth

name	required	NULL allowed	type	description
Id	yes	yes	Int64	Record ID. Example: 1
Month	yes	yes	String	Month. The format should be yyyy-mm, for example, 2021-01. Example: 2021-01
TotalCost	yes	yes	Float	Consumed amount. Example: 12.23
GrowthRate	yes	yes	String	Growth rate compared to last month (%). Positive values indicate an increase, negative values indicate a decrease, and an empty value indicates that the growth rate cannot be calculated. Example: 24

MemberNodes

Referenced by the following interfaces: DescribeOrganizationMemberNodes

name	required	NULL allowed	type	description
MemberUin	yes	yes	Int64	Member UIN. Example: 111111111111
Nodes	yes	yes	Array of OrgNode	Node list. Example:View

FinancialMemberNum

Referenced by the following interfaces: DescribeOrganizationFinancialMemberNum

name	required	NULL allowed	type	description
SelfPayNoInherit	yes	yes	Int64	Number of self-paying members who have not inherited the discount. Example: 3

name	required	NULL allowed	type	description
SelfPayInherit	yes	yes	Int64	Number of self-paying members who have inherited the discount. Example: 2
AuthName	yes	yes	String	Entity Name Example: auth_name
AuthType	yes	yes	String	Entity type. manager: administrator; member: member. Example: manager
PayUin	yes	yes	String	Paid-on-behalf accounts Example: 111111111111
BehalfPay	yes	yes	Int64	Number of members with proxy payment. Example: 2

OrgMemberFinancial

Referenced by the following interfaces: DescribeOrganizationFinancialByMember

name	required	NULL allowed	type	description
MemberUin	yes	yes	Int64	Member UIN. Example: 1000001
MemberName	yes	yes	String	Member name. Example: member_name
TotalCost	yes	yes	Float	Consumed amount. Example: 20.23
Ratio	yes	yes	String	Percentage. Example: 23

Tags

Referenced by the following interfaces: DescribeAllParentNodes, DescribeOrganizationMember, DescribeOrganizationMemberNodes, DescribeOrganizationMembers, DescribeOrganizationNode, DescribeOrganizationNodeByName, DescribeOrganizationNodeMembers, DescribeOrganizationNodes, DescribeOrganizationNodesByParent

name	required	NULL allowed	type	description
TagKey	yes	yes	String	Tag key. Example: key
TagValue	yes	yes	String	Tag value. Example: value

OrgCreateRecord

Referenced by the following interfaces: DescribeOrganizationCreateRecord, DescribeOrganizationPendingCreateRecord

name	required	NULL allowed	type	description
OrgPermission	yes	yes	Array of OrgPermission	Policy Authorization Example:View
ApplyTime	yes	yes	String	Application time Example: ""
ApprovalTime	yes	yes	String	Review time Example: ""
Id	yes	no	Uint64	Invitation ID. Example: 100
OrgPolicyType	yes	yes	String	Relationship policy type. Example: Finical
OrgPolicyName	yes	yes	String	Relational policy name. Example: Financial management
CreateTime	yes	yes	String	Creation Time Example: 2021-01-23 09:11:11
PayUin	yes	yes	String	Proxy payer UIN. Example: ""
ApprovalUin	yes	yes	Int64	Approver account. Example: 0
Name	yes	yes	String	Invited member name. Example: member_name
HostUin	yes	yes	Int64	Administrator UIN Example: 1000002
NodeId	yes	yes	Int64	Node ID. Example: 1000
Remark	yes	yes	String	Remarks Example: remark
UpdateTime	yes	yes	String	Update time Example: 2021-01-23 09:11:11
AccountName	yes	yes	String	Account name Example: account_name
Reason	yes	yes	String	Failure reason Example: Failed to create the account
PayName	yes	yes	String	Proxy payer name. Example: ""

name	required	NULL allowed	type	description
MemberUin	yes	yes	Int64	Invited member UIN. Example: 1000001
Status	yes	yes	String	Invitation status. Valid; Accepted; Denied; Canceled; InValid. Example: Cancel
OrgType	yes	yes	Uint64	Organization Type Example: 1
NodeName	yes	yes	String	Node name. Example: node_name
OrgIdentity	yes	yes	Array of MemberIdentity	Management identity Example:View

MemberMainInfo

Referenced by the following interfaces: DescribeOrganizationAuthPolicies, DescribeOrganizationMembersAuthPolicy

name	required	NULL allowed	type	description
MemberName	yes	yes	String	Member name. Example: member_name
MemberUin	yes	yes	Int64	Member UIN Example: 100000000001

OrgAuthPolicy

Referenced by the following interfaces: DescribeOrganizationAuthPolicies

name	required	NULL allowed	type	description
AuthSubAccounts	yes	yes	Array of OrgAuthSubAccount	Associated sub-account. Example:View
AuthGroups	yes	yes	Array of AuthGroup	Associated user group. Example:View
IdentityRoleName	yes	yes	String	Role name of an identity. Example: role_name
Description	yes	yes	String	Description. Example: description
CreateTime	yes	yes	String	Creation time. Example: 2021-02-12 12:12:10
Members	yes	yes	Array of MemberMainInfo	Authorized member. Example:View
UpdateTime	yes	yes	String	Update time. Example: 2021-02-12 12:12:10
PolicyId	yes	yes	Int64	Policy ID. Example: 10
PolicyName	yes	yes	String	Policy name. Example: policy_name
IdentityId	yes	yes	Int64	Identity ID. Example: 1
IdentityRoleAliasName	yes	yes	String	Role alias of an identity. Example: alias_name

OrgCollPolicy

Referenced by the following interfaces: DescribeOrganizationCollPolicies

name	required	NULL allowed	type	description
PolicyName	yes	yes	String	Policy name. Example: policy_name
IdentityId	yes	yes	Int64	Identity ID. Example: 1
IdentityRoleName	yes	yes	String	Identity role name. Example: role_anme
IdentityRoleAliasName	yes	yes	String	Role alias of an identity. Example: alias_name
CreateTime	yes	yes	String	Creation time. Example: 2021-02-12 12:12:10
UpdateTime	yes	yes	String	Update time. Example: 2021-02-12 12:12:10
PolicyId	yes	yes	Int64	Policy ID. Example: 1000001

NotAllowReason

Referenced by the following interfaces: CheckAccountDelete

name	required	NULL allowed	type	description

name	required	NULL allowed	type	description
IsCreateMember	yes	yes	Bool	Specifies whether a member is a created one. true: yes; false: no. Members that are not created cannot be deleted. Example: true
DeletionPermission	yes	yes	Bool	Member deletion permission. true: enabled; false: disabled. Deletion is not allowed when member deletion permission is disabled. Example: true
IsShareManager	yes	yes	Bool	Specifies whether a member is a shared resource administrator. true: yes; false: no. Members who are shared resource administrators cannot be deleted. Example: false
OperateProcess	yes	yes	Bool	Specifies whether a member has set up operation approval. true: yes; false: no. Members who have set up operation approval cannot be deleted. Example: false
IsAssignManager	yes	yes	Bool	Specifies whether a member is a delegated trusted service administrator. true: yes; false: no. Members who are delegated trusted service administrators cannot be deleted. Example: false
IsAuthManager	yes	yes	Bool	Specifies whether a member is an entity administrator. true: yes; false: no. Members who are entity administrator cannot be deleted. Example: false
BillingPermission	yes	yes	Bool	Specifies whether revocation of members' financial permissions is allowed. true: yes; false: no. Members cannot be deleted if their financial permissions cannot be revoked. Example: true
ExistResources	yes	yes	Array of String	List of existing resources. Accounts with resources cannot be deleted. Example: ["cvm"]
DetectFailedResources	yes	yes	Array of String	List of resources with detection failures. Deletion is not allowed if an account has resources with detection failures. Example: ["cvm"]

ListPoliciesForTarget

Referenced by the following interfaces: ListPoliciesForTarget

name	required	NULL allowed	type	description
Remark	yes	yes	String	Remark Example: Dedicated for self-test
Uin	yes	no	Uint64	Associated account or node. Example: 15440611
AddTime	yes	yes	String	Policy creation time Example: 2022-08-08 14:49:59
AttachTime	yes	yes	String	Policy binding time. Example: 2022-08-08 14:49:59
StrategyId	yes	no	Uint64	Policy ID Example: 1000
StrategyName	yes	no	String	Policy Name Example: FullQcloudAccess
Type	yes	no	Uint64	Association type. 1: node association; 2: user association. Example: 1
UpdateTime	yes	yes	String	Policy Update Time Example: 2022-08-08 14:49:59
Name	yes	yes	String	Department Name Example: Secondary Department

OrgBeInviteRecord

Referenced by the following interfaces: DescribeOrganizationBeInviteRecord

name	required	NULL allowed	type	description
OrgPermission	yes	yes	Array of OrgPermission	Policy Authorization Example:View
CreateTime	yes	yes	String	Creation Time Example: 2021-01-23 09:11:11
ExpireTime	yes	yes	String	Expiration Time Example: 2021-01-23 09:11:11
HostName	yes	yes	String	Administrator nickname. Example: host_name
OrgType	yes	yes	Int64	Organization Type Example: 1
OrgId	yes	yes	Int64	Organization ID Example: 11
PayUin	yes	yes	String	Proxy payer UIN. Example: ""
MemberUin	yes	yes	Int64	Invited member UIN. Example: 1000001
Name	yes	yes	String	Invited member name. Example: member_name
OrgPolicyType	yes	yes	String	Relationship policy type. Example: Finical
OrgPolicyName	yes	yes	String	Relational policy name. Example: Financial management
IsAllowQuit	yes	yes	String	Whether to allow a member to exit. Valid values: Allow, Denied. Example: Allow
Id	yes	no	Uint64	Invitation ID. Example: 100

name	required	NULL allowed	type	description
HostUin	yes	yes	Int64	Administrator UIN Example: 1000002
PayName	yes	yes	String	Proxy payer name. Example: ""
Status	yes	yes	String	Invitation status. Valid; Accepted; Denied; Canceled; InValid. Example: Cancel
NodeId	yes	yes	Int64	Node ID. Example: 1000
Remark	yes	yes	String	Remarks Example: remark

OrgPermission

Referenced by the following interfaces: DescribeMemberBeChangePermissionRecords, DescribeMemberChangePermissionRecords, DescribeOrganizationBeInviteRecord, DescribeOrganizationCreateRecord, DescribeOrganizationInviteRecord, DescribeOrganizationPendingCreateRecord

name	required	NULL allowed	type	description
Id	yes	no	Uint64	Permission ID. Example: 1
Name	yes	no	String	permission name Example: Allow the root account to merge bills for sub-accounts.

AccountStatus

Referenced by the following interfaces: CheckAccountStatus

name	required	NULL allowed	type	description
AccountUin	yes	yes	Int64	Root account UIN. Example: 111111111111
SameOrganization	yes	yes	Bool	Specifies whether an account is in the same organization as the current account. true: yes; false: no. Example: false
SameAuth	yes	yes	Bool	Specifies whether an account belongs to the same real-name entity as the current account. true: yes; false: no. Example: false
OtherOrganization	yes	yes	Bool	Specifies whether an account is in an organization different from the current account. true: yes; false: no. Example: false
DistributionAccount	no	yes	Bool	Specifies whether an account belongs to a reseller. true: yes; false: no. Example: false

NodeMember

Node Member User

Referenced by the following interfaces: DescribeOrganizationNodeMembers

name	required	NULL allowed	type	description
MemberUin	no	no	Int64	Member Account UIN Example: 111111111111
Name	no	no	String	Name Example: member_name
Remark	no	no	String	Remarks Example: ""
MemberType	no	no	String	Member Type, Create, Invite, Admin, etc Example: Invite
OrgPolicyType	no	no	String	Organization Policy Type, Finance Example: 1
OrgPermission	no	no	Array of Permission	Permission List Example:View
PayUin	no	no	String	Pay-on-Behalf Account Example: 111111111111
PayName	no	no	String	Pay-on-Behalf Username Example: member_name
CreateTime	no	no	String	Creation Time Example: 2021-11-12 12:09:08
OrgIdentities	no	no	Array of MemberIdentity	Member access permission Example:View
Tags	no	no	Array of Tags	Member tag list. Example:View

OrgSubAccountByMonth

Referenced by the following interfaces: DescribeOrganizationSubAccountByMonth

name	required	NULL allowed	type	description
Id	yes	yes	Int64	Record ID. Example: 1

name	required	NULL allowed	type	description
Month	yes	yes	String	Month. The format should be yyyy-mm, for example, 2021-06. Example: 2021-01
SubAccountNum	yes	yes	Int64	Total number of sub-accounts for the current month. Example: 11
MemberNum	yes	yes	Int64	Total number of members in the current month. Example: 10

OrgInvitation

Referenced by the following interfaces: DescribeOrganizationInviteRecord

name	required	NULL allowed	type	description
MemberUin	yes	yes	Int64	Invited member UIN. Example: 1000001
Name	yes	yes	String	Invited member name. Example: member_name
Status	yes	yes	String	Invitation status. Valid; Accepted; Denied; Canceled; InValid; Pending. Example: Cancel
OrgType	yes	yes	Uint64	Organization Type Example: 1
ExpireTime	yes	yes	String	Expiration Time Example: 2021-01-23 09:11:11
OrgPolicyType	yes	yes	String	Relationship policy type. Example: Financial
OrgPermission	yes	yes	Array of OrgPermission	Policy Authorization Example:View
NodeName	yes	yes	String	Node name. Example: node_name
PayUin	yes	yes	String	Proxy payer UIN. Example: 100000000001
Id	yes	no	Uint64	Invitation ID. Example: 100
HostUin	yes	yes	Int64	Administrator UIN Example: 1000002
NodeId	yes	yes	Int64	Node ID. Example: 1000
OrgPolicyName	yes	yes	String	Relational policy name. Example: Financial management
CreateTime	yes	yes	String	Creation Time Example: 2021-01-23 09:11:11
JoinTime	yes	yes	String	Join time Example: 2021-01-23 09:11:11
Remark	yes	yes	String	Remarks Example: invitation member
IsAllowQuit	yes	yes	String	Specifies whether members are allowed to exit. Allow: yes; Denied: no. Example: Allow
PayName	yes	yes	String	Proxy payer name. Example: host_name

SubAccountInfo

Referenced by the following interfaces: ListOrgMemberSubAccount

name	required	NULL allowed	type	description
CanLogin	yes	no	Uint64	Specifies whether an account can log in to the console. 1: yes; 0: no. Example: 1
Phone	yes	no	String	Mobile phone number Example: 1******54
Email	yes	no	String	Email address Example: e*******.com
CreateTime	yes	no	String	Creation Time Example: 2022-03-12 12:12:54
SubUin	yes	yes	String	Sub-account UIN Example: 11111111111
DepartmentName	yes	no	String	Department Example: node_name
MemberName	yes	yes	String	Name Example: member_namer
RoleName	yes	no	String	Roles Example: Development
Remark	no	yes	String	Member account description. Example: Member 1
SubName	yes	yes	String	Sub-account name Example: sub_name

name	required	NULL allowed	type	description
MemberUin	yes	yes	String	Member Account UIN Example: 222222222222

MemberPermissionChangeRecord

Referenced by the following interfaces: DescribeMemberBeChangePermissionRecords, DescribeMemberChangePermissionRecords

name	required	NULL allowed	type	description
Status	yes	no	String	Change status. Valid: pending confirmation; Accept: effective; Denied: rejected; Canceled: canceled; InValid: expired. Example: Valid
NewOrgPermission	yes	no	Array of OrgPermission	Permissions after change. Example:View
HostUin	yes	no	Uint64	Administrator UIN Example: 122
NewPayUin	yes	yes	String	Proxy payer after change. Example: 233
CreateTime	yes	no	String	Submitted at Example: 2021-11-29 09:08:12
OldOrgPermission	yes	no	Array of OrgPermission	Permissions before change. Example:View
ExpireTime	yes	no	String	End time Example: 2021-12-29 09:08:12
OldPayUin	yes	yes	String	Proxy payer before change. Example: **
OldPayName	yes	yes	String	Proxy payer name before change. Example: **
NewPayName	yes	yes	String	Proxy payer name after change. Example: tee
Operator	yes	no	String	Operator Example: aeq
Id	yes	no	Uint64	Record ID Example: 1221
MemberUin	yes	no	Uint64	Member UIN. Example: 100000001
Name	yes	no	String	Member Name Example: member_name

OrgRecord

Referenced by the following interfaces: DescribeOrganizationRecords

name	required	NULL allowed	type	description
Status	yes	yes	String	Invitation status. Valid; Accepted; Denied; Canceled; InValid; Success; Failed. Example: Cancel
RecordType	yes	yes	String	Record type. Invite: invitation; Create: creation; Quit: quitting; Delete: deletion. Example: Finical
Remark	yes	yes	String	Remarks Example: 2021-01-23 09:11:11
CreateTime	yes	yes	String	Creation Time Example: 2021-01-23 09:11:11
UpdateTime	yes	yes	String	Expiration Time Example: 2021-01-23 09:11:11
Id	yes	no	Uint64	Invitation ID. Example: 100
MemberUin	yes	yes	Int64	Invited member UIN. Example: 1000001
Name	yes	yes	String	Invited member name. Example: member_name

AuthGroup

Referenced by the following interfaces: DescribeOrganizationAuthPolicies

name	required	NULL allowed	type	description
GroupId	yes	yes	Uint64	User group ID. Example: 111
GroupName	yes	yes	String	User group name. Example: group_name

OrgAuthSubAccount

Referenced by the following interfaces: DescribeOrganizationAuthPolicies

name	required	NULL allowed	type	description

name	required	NULL allowed	type	description
SubAccountUin	yes	yes	Uint64	Sub-account UIN. Example: 111111111111
SubAccountName	yes	yes	String	Sub-account username. Example: sub_name

OrgMembersAuthPolicy

Referenced by the following interfaces: DescribeOrganizationMembersAuthPolicy

name	required	NULL allowed	type	description
MemberName	yes	yes	String	Member name. Example: member-name
BindType	yes	yes	Uint64	Binding type. 1: sub-account; 2: user group. Example: 1
IdentityId	yes	yes	Int64	Identity ID. Example: 111
IdentityRoleName	yes	yes	String	Role name of an identity. Example: role_name
IdentityRoleAliasName	yes	yes	String	Role alias of an identity. Example: alias_name
MemberUin	yes	yes	Int64	Member UIN. Example: 111111111111
OrgSubAccountName	yes	yes	String	Sub-account name or user group name. Example: sub-name
Members	no	yes	Array of MemberMainInfo	Member information. Example:View
CreateTime	yes	yes	String	Creation time. Example: 2021-02-12 12:12:10
PolicyId	yes	yes	Int64	Member access policy ID. Example: 222
PolicyName	yes	yes	String	Member access policy name. Example: policy_name
OrgSubAccountUin	yes	yes	Int64	Sub-account UIN or user group ID. Example: 222222222222

OrgMemberAuthAccount

Sub-account Authorized by Member

Referenced by the following interfaces: DescribeOrganizationMemberAuthAccounts

name	required	NULL allowed	type	description
OrgSubAccountUin	yes	no	Uint64	Sub-account UIN Example: 1000001
PolicyId	no	no	Int64	Policy ID Example: 1001
PolicyName	no	no	String	Policy Name Example: policy_name
IdentityId	no	no	Int64	Identity ID Example: 12
IdentityRoleName	no	no	String	Identity Role Name Example: identity_role
IdentityRoleAliasName	no	no	String	Identity Role Alias Example: Policy Management
CreateTime	no	no	String	Creation Time Example: 2021-02-12 12:12:10
UpdateTime	no	no	String	Update time Example: 2021-02-12 12:12:10
MemberUin	no	no	Uint64	Authorized Member Account UIN Example: 111111111111

MemberIdentity

Referenced by the following interfaces: DescribeOrganizationCreateRecord, DescribeOrganizationNodeMembers, DescribeOrganizationPendingCreateRecord

name	required	NULL allowed	type	description
IdentityId	yes	yes	Int64	Identity ID. Example: 10
IdentityAliasName	yes	yes	String	Identity name. Example: identity_name

StatusInfo

Referenced by the following interfaces: CreateOrganizationMembers

name	required	NULL allowed	type	description

name	required	NULL allowed	type	description
MemberUin	yes	no	Int64	Member UIN. Example: 1000001
Code	yes	no	String	Status code. Success: success Example: Success
Message	yes	no	String	Descriptions Example: Success

OrgMembersAuthAccount

Referenced by the following interfaces: DescribeOrganizationMembersAuthAccount

name	required	NULL allowed	type	description
MemberUin	yes	yes	Int64	Member UIN. Example: 111111111111
MemberName	yes	yes	String	Member name. Example: member-name
OrgSubAccountUin	yes	yes	Int64	Organization administrator sub-account UIN. Example: 222222222222
OrgSubAccountName	yes	yes	String	Organization administrator sub-account name. Example: sub-name
AuthPolicies	yes	yes	Array of OrgMemberPolicy	Member access policy list. Example:View

NodeTag

Referenced by the following interfaces: AddOrganizationNodeTags, DescribeOrganizationNodeTags

name	required	NULL allowed	type	description
TagKey	no	yes	String	Tag Key Example: 1001
TagValue	no	yes	String	Tag Value Example: 345

OrgMemberAuthIdentity

Referenced by the following interfaces: DescribeOrganizationMemberAuthIdentities, DescribeOrganizationMembersCanAuthIdentities

name	required	NULL allowed	type	description
IdentityId	yes	yes	Int64	Identity ID. Example: 1
IdentityRoleAliasName	yes	yes	String	Role alias of an identity. Example: identity_name
Description	yes	yes	String	Identity description. Example: admin identity
UpdateTime	yes	yes	String	Time of the last successful configuration. Example: 2021-02-12 12:12:10
Status	no	yes	Uint64	Configuration status. Valid values: 1: configuration completed; 2: reconfiguration required. Example: 1
MemberUin	no	yes	Int64	Member UIN. Example: 1111111111111
MemberName	no	yes	String	Member name. Example: member_name
IdentityRoleName	yes	yes	String	Role name of an identity. Example: identity_role
CreateTime	yes	yes	String	Time of initial configuration success. Example: 2021-02-12 12:12:10
IdentityType	yes	yes	Uint64	Identity type. Valid values: 1: preset identity; 2: custom identity. Example: 1

OrgIdentity

Referenced by the following interfaces: ListOrganizationIdentity

name	required	NULL allowed	type	description
IdentityType	yes	yes	Uint64	Identity type. 1: preset; 2: custom. Example: 1
UpdateTime	yes	yes	String	Update time. Example: 2021-02-12 12:12:10
Status	no	yes	Uint64	Configuration status. Valid values: 1: configuration completed; 2: reconfiguration required. Example: 1
IdentityId	yes	yes	Int64	Identity ID. Example: 10
IdentityAliasName	yes	yes	String	Identity name. Example: identity_name

name	required	NULL allowed	type	description
Description	yes	yes	String	Description. Example: admin identity
IdentityPolicy	yes	yes	Array of IdentityPolicy	Identity policy. Example:View

ErrorCode

Feature Description

If there is an Error field in the response, it means that the API call failed. For example:

```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```

Code in Error indicates the error code, and Message indicates the specific information of the error.

Error Code List

Common Error Codes

Error codes	Description
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	Key does not exist. Check if the key has been deleted or disabled in the console, and if not, check if the key is correctly entered. Note that whitespaces should not exist before or after the key.
AuthFailure.SignatureExpire	Signature expired. Timestamp and server time cannot differ by more than five minutes. Please ensure your current local time matches the standard time.
AuthFailure.SignatureFailure	Invalid signature. Signature calculation error. Please ensure you've followed the signature calculation process described in the Signature API documentation.
AuthFailure.TokenFailure	Token error.

Error codes	Description
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	HTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

Service Error Codes

Error codes	Description
FailedOperation.ReSentInvitation	

Error codes	Description
ResourceNotFound.OrganizationNodeNotExist	The organization node does not exist.
FailedOperation.PartnerManagementErr	
InvalidParameter.OrganizationMemberNotManager	
UnsupportedOperation.DeleteDelegatePayerNotAllow	
FailedOperation.OrganizationPolicyIsNotDisabled	
LimitExceeded.SendEmailLimit	
UnsupportedOperation.CreateMemberNotAllowCreateOrganization	
InvalidParameter.AllowQuitIllegal	
UnsupportedOperation.MemberAccountExistResource	
FailedOperation.ChangePermissionRecordExist	
FailedOperation.MemberBindEmailError	
LimitExceeded.OrganizationMemberOverLimit	
UnsupportedOperation.MemberDiscountInheritExisted	
FailedOperation.CreateAccount	
ResourceNotFound.OrganizationNotExist	The organization does not exist.
ResourceNotFound.ChangePermissionNotExist	
FailedOperation.MemberIsDelegatePayerNotAllowDelete	
FailedOperation.OrganizationAuthRelationExist	
FailedOperation.ExistOtherOrganizationMemberShared	
FailedOperation.OperateBillingPermissionErr	
LimitExceeded.NodeDepthExceedLimit	The node depth exceeds the limit.
FailedOperation	
FailedOperation.BindEmailLinkExpired	

Error codes	Description
FailedOperation.CreateBillingPermissionErr	
FailedOperation.OrganizationIdentityInUsed	
UnsupportedOperation.OwnerDiscountInheritExisted	
ResourceNotFound.OrganizationIdentityNotExist	
UnsupportedOperation.MemberExistOperateProcessNotAllowDelete	
FailedOperation.ImportFileIllegal	
FailedOperation.CreateRecordNotExist	
InvalidParameter.InterfaceNotExist	
UnsupportedOperation.AddDiscountInheritNotAllow	
FailedOperation.AddGrant	
LimitExceeded.OrgServiceEnableLimit	
LimitExceeded.SendFrequency	
FailedOperation.QuitShareUint	
LimitExceeded.UpdateEmailBindOverLimit	
FailedOperation.GetPolicyDetail	
FailedOperation.SubAccountNotExist	
InternalError.SystemError	Internal system exception
ResourceNotFound.ShareResourceMemberNotExist	
FailedOperation.GetSubAccountListError	
LimitExceeded.CreateMemberOverLimit	
ResourceNotFound.NotFound	
InvalidParameter.DescriptionOverLimit	The description exceeds the length limit.
FailedOperation.MemberEmailExist	
InvalidParameter.CodeExpired	

Error codes	Description
FailedOperation.OrganizationAuthManageNotAllowDelete	
FailedOperation.NotSameRegion	
FailedOperation.QuitShareUintError	
LimitExceeded.InvitationOverLimit	
FailedOperation.ChangePermissionInvalid	
InvalidParameter.OrganizationMemberNotExist	
FailedOperation.MemberPolicyNameExist	
FailedOperation.AuthNotEnterprise	
MissingParameter	
UnsupportedOperation.SecondaryDistributorSubClientExisted	
FailedOperation.CreateMemberAuthOverLimit	
FailedOperation.DisableDeleteMemberFromRootNode	Prohibited to delete members from the root node.
InvalidParameter.ParamError	Parameter error
UnsupportedOperation.OrderInProgressExisted	
InvalidParameter.InvalidEmail	
ResourceNotFound.UserNotExist	
UnsupportedOperation.MemberIsNotClient	
ResourceNotFound.OrganizationAuthRelationNotExist	
FailedOperation.MemberExistInOtherOrganization	
FailedOperation.MemberExistDelegatePayerNotAllowDelete	
InvalidParameter.OrganizationNotExist	
ResourceNotFound.SomeUinsNotInOrganization	The account is not within the organization.
FailedOperation.OrganizationPolicyIllegal	
FailedOperation.QuiteShareUnit	

Error codes	Description
InvalidParameter	
FailedOperation.GetAccountRegion	
FailedOperation.OrganizationIdentityNameUsed	
LimitExceeded.PhoneNumBound	
FailedOperation.OrganizationNodeNameUsed	The node name has already been used.
UnsupportedOperation.MemberExistAccountLevelDiscountInherit	
ResourceNotFound.InvitationNotExist	
InvalidParameter.CodeError	
FailedOperation.OrganizationMemberNameUsed	
UnsupportedOperation.AddDelegatePayerNotAllow	
FailedOperation.AccountAlreadyRegister	
FailedOperation.GetAuthInfo	
ResourceNotFound.OrganizationServiceNotExist	
ResourceNotFound.MemberOperateProcessNotExist	
FailedOperation.OperatePolicy	Policy authorization failed.
ResourceNotFound.EmailBindRecordNotExist	
ResourceNotFound.ApplyNotExist	
LimitExceeded.IdentityExceedLimit	
ResourceNotFound.ResourceTypeNotExist	
UnsupportedOperation.CreateMemberNotAllowDelete	
LimitExceeded.EmailBindOverLimit	
UnsupportedOperation.InviteAccountNotAllowDelete	
FailedOperation.GroupNotExist	
ResourceNotFound.OrganizationMemberNotExist	The member account does not exist.

Error codes	Description
FailedOperation.OrganizationIdentityPolicyError	
UnsupportedOperation.MemberNoPayment	
LimitExceeded.NodeTageOverLimit	
FailedOperation.CheckMailAccount	
InvalidParameter.CodeVerified	
FailedOperation.OrganizationMemberExist	
UnsupportedOperation.AbnormalFinancialStatusOfAdmin	
UnsupportedOperation.CreateMemberNotAllowQuit	
FailedOperation.EmailBindRecordInvalid	
FailedOperation.ApplyExist	
InvalidParameter.PasswordIllegal	
FailedOperation.PayUinIllegal	
UnsupportedOperation.AgentNotSame	
FailedOperation.OrganizationNodeNotExist	
UnsupportedOperation.MemberAccountArrears	
FailedOperation.DisableQuitSelfCreatedOrganization	
FailedOperation.MemberIdentityAuthUsed	
ResourceNotFound.MemberPolicyNotExist	Policy authorization does not exist.
FailedOperation.AuthInfoNotSame	
LimitExceeded.OrganizationNodeDeleteOverLimit	Exceed maximum number of deleted nodes.
FailedOperation.ShareResourceMemberInUse	
FailedOperation.CreatePolicy	
FailedOperation.CreateProductRoleNotAllow	
FailedOperation.MemberNameUsed	

Error codes	Description
FailedOperation.MemberShareResource	
FailedOperation.MemberBindPhoneError	
FailedOperation.BindEmailLinkInvalid	
FailedOperation.InvitationInvalid	
FailedOperation.EmailAlreadyUsed	
FailedOperation.CheckAccountPhoneBindLimit	
UnsupportedOperation.AbnormalFinancialStatusOfMember	
ResourceNotFound.MemberNotExist	
UnsupportedOperation.MemberNotAllowQuit	
FailedOperation.OrganizationNodeNotEmpty	Organization node is not empty.
ResourceNotFound.NodeNotExist	
FailedOperation.OrganizationExistAlready	
UnsupportedOperation	
UnsupportedOperation.PayerExistAccountLevelDiscountInherit	
UnsupportedOperation.MemberExistServiceNotAllowDelete	
UnsupportedOperation.ExistedClient	
LimitExceeded.NodeExceedLimit	The number of nodes exceeds the limit.
FailedOperation.InvitationExist	
FailedOperation.CreateRecordAlreadySuccess	
LimitExceeded.SendEmailWithinOneHourLimit	
ResourceNotFound.MemberEventNotExist	
ResourceNotFound.OrganizationServiceAssignNotExist	
UnsupportedOperation.MemberHasVoucher	
InvalidParameter.ImageCodeError	

Error codes	Description
FailedOperation.ShareUnitNotEmpty	
FailedOperation.CertificateVerificationFailed	The qualification approval is not passed.
ResourceNotFound.MemberIdentityNotExist	The member role identity does not exist.
UnsupportedOperation.PayerArrearsAndNoCreditAccount	
FailedOperation.DeletePolicy	
ResourceUnavailable	
InternalError	
InvalidParameter.OrganizationNodeNotExist	
UnsupportedOperation.ManagementSystemError	
UnsupportedOperation.MemberIsAgent	
FailedOperation.AuthInfoEmpty	
FailedOperation.OrganizationPermissionIllegal	
UnsupportedOperation.ExistedAgent	
FailedOperation.OrganizationNotEmpty	
ResourceNotFound.PolicyNotExist	
ResourceNotFound.PolicyIdNotFound	
UnsupportedOperation.DeleteAccountDisabled	
LimitExceeded.Members	
ResourceNotFound.ServiceRoleNotExist	
FailedOperation.CreateRole	
UnsupportedOperation.InconsistentUserTypes	