Cloud Access Management

User Guide

Copyright Notice

Trademark Notice

Tencent Cloud

Service Notice

This document provides an overview of the as–is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

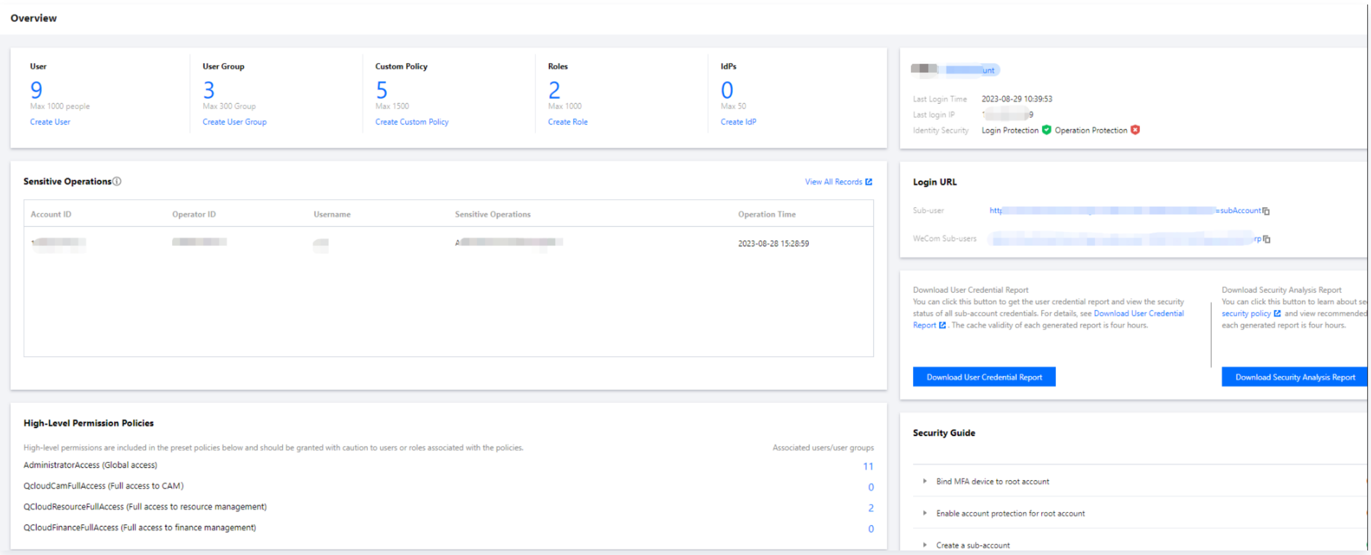
We are committed to providing personalized pre–sales consultation and technical after–sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

User Guide
Overview

Last updated：2023-08-31 17:01:36

The Overview page of the Cloud Access Management Console comprises seven major modules: **Access Management Resources**, **Login URL**, **Sensitive Operations**, **High-Level Permission Policies**, **Last Login Information**, **Security Analysis Report**, and **Security Guide**.



Overview

User
9
Max 1000 people
Create User

User Group
3
Max 300 Group
Create User Group

Custom Policy
5
Max 1500
Create Custom Policy

Roles
2
Max 1000
Create Role

IdPs
0
Max 50
Create IdP

[redacted]unt

Last Login Time 2023-08-29 10:39:53
Last login IP [redacted]
Identity Security Login Protection ✓ Operation Protection ✗

Sensitive Operations ⓘ View All Records

Account ID	Operator ID	Username	Sensitive Operations	Operation Time
[redacted]	[redacted]	[redacted]	[redacted]	2023-08-28 15:28:59

Login URL

Sub-user [redacted]=subAccount
WeCom Sub-users [redacted]rp

Download User Credential Report
You can click this button to get the user credential report and view the security status of all sub-account credentials. For details, see Download User Credential Report. The cache validity of each generated report is four hours.

Download User Credential Report

Download Security Analysis Report
You can click this button to learn about se
security policy and view recommended
each generated report is four hours.

Download Security Analysis Report

High-Level Permission Policies

High-level permissions are included in the preset policies below and should be granted with caution to users or roles associated with the policies.

	Associated users/user groups
AdministratorAccess (Global access)	11
QcloudCamFullAccess (Full access to CAM)	0
QCloudResourceFullAccess (Full access to resource management)	2
QCloudFinanceFullAccess (Full access to finance management)	0

Security Guide

- Bind MFA device to root account
- Enable account protection for root account
- Create a sub-account

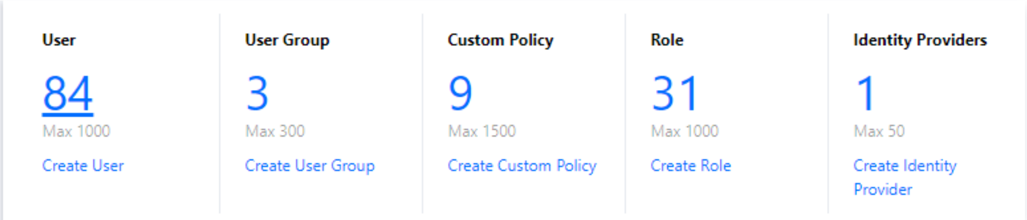
Overview Page Permission

- Users with **QcloudCamSummaryAccess policy permissions** can log in to the console and view information from all modules.
- Users without **QcloudCamSummaryAccess policy permissions** can only view **Login URL** and **Last Login Information** when logging into the console.
- The root account and administrator users (AdministratorAccess) already include this policy permission.
- Sub-accounts can contact the root account to check whether they have QcloudCamSummaryAccess policy permissions on the User List > **User Details** page.
- The root account can grant QcloudCamSummaryAccess policy to the necessary sub-accounts, allowing them to view all information on the console overview page. For the authorization method, please refer to Authorization Management.

Overview Page Modules

CAM Resources

The Access Management Resources module displays the number of users, user groups, custom policies, roles, and identity providers created under the current root account. You can enter the corresponding creation page by clicking the button below the number.



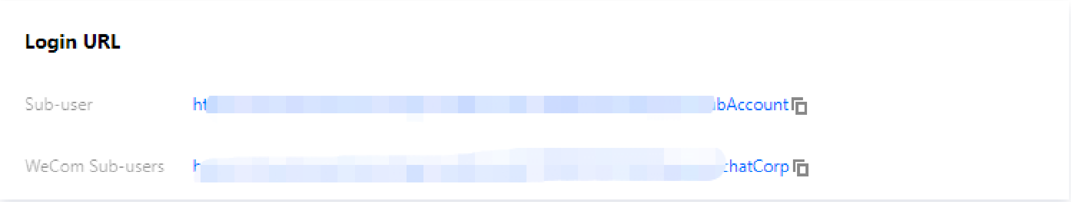
User	User Group	Custom Policy	Role	Identity Providers
84	3	9	31	1
Max 1000	Max 300	Max 1500	Max 1000	Max 50
Create User	Create User Group	Create Custom Policy	Create Role	Create Identity Provider

Login URL

The Login URL module displays the login links for sub-users and WeCom sub-users. Both the root account and sub-accounts can copy the link using the copy button on the right side of the link.

- Sub-user Login Link: Applicable to sub-users.

- WeCom Sub-user Login Link: Applicable to sub-users created and associated via WeCom.



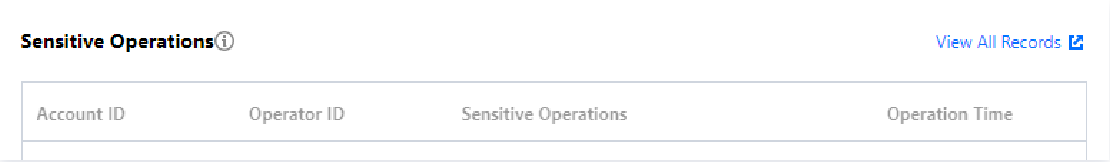
Login URL

Sub-user ht[redacted]bAccount

WeCom Sub-users h[redacted]hatCorp

Sensitive Operations

The Sensitive Operations module displays an overview of all sensitive operations (up to 50) under the current root account in the last 3 days. The displayed information includes: Account ID, Operator ID, Detailed Sensitive Operations, and Operation Time. Users can also view more detailed sensitive operation records in the CloudAudit console by clicking on **View All Records**.

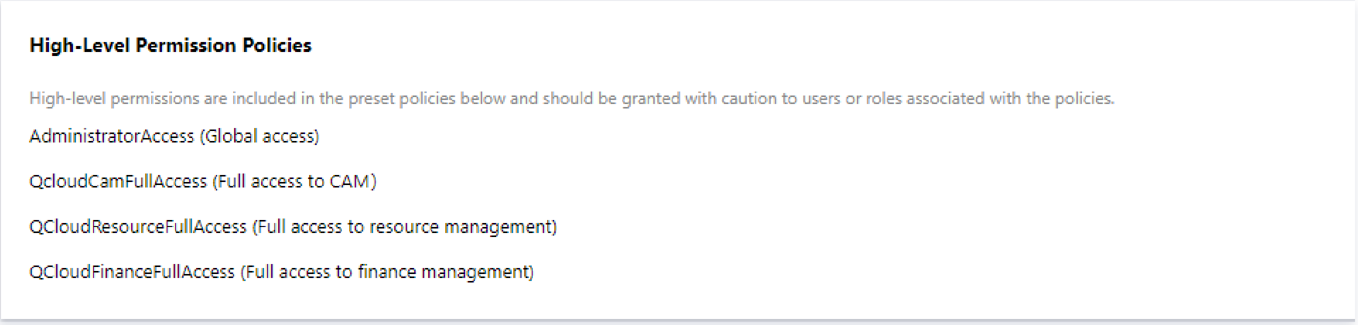


Sensitive Operationsⓘ

Account ID	Operator ID	Sensitive Operations	Operation Time

High-Level Permission Policies

The High-Level Permission Policies module lists preset policies with elevated permissions. It is crucial to monitor users or roles associated with these high privilege policies and allocate permissions appropriately.



High-Level Permission Policies

High-level permissions are included in the preset policies below and should be granted with caution to users or roles associated with the policies.

AdministratorAccess (Global access)

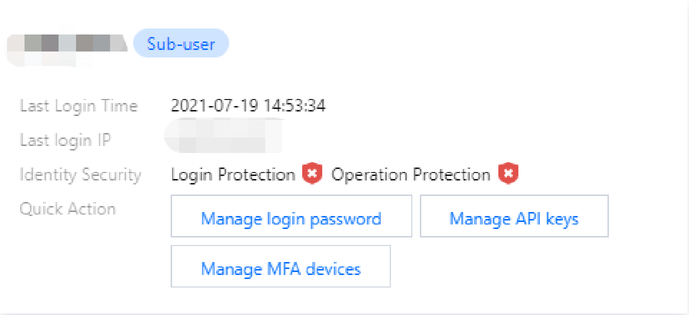
QcloudCamFullAccess (Full access to CAM)

QCloudResourceFullAccess (Full access to resource management)

QCloudFinanceFullAccess (Full access to finance management)

Last login information

The Last Login Information module displays the last login time, last login IP, and identity security status of the current account.



[redacted] Sub-user

Last Login Time 2021-07-19 14:53:34

Last login IP [redacted]

Identity Security Login Protection ☒ Operation Protection ☒

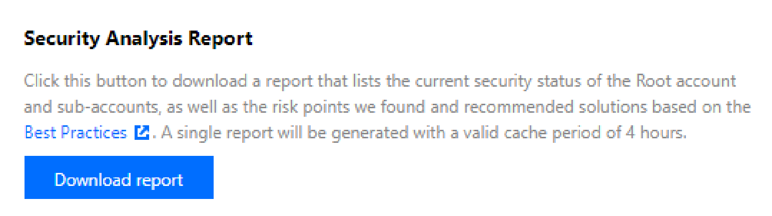
Quick Action

Download report

The Download Report module offers the functionality to download User Credential Reports and Security Analysis Reports. You can click the download button to obtain the corresponding report content. The cache validity period for a single report generation is 4 hours.

- User Credential Report: This report records the status of all sub-accounts and their user credentials under the current account, such as basic account information, console login status, access keys, and account security settings. You can use this report for compliance auditing.
- Security Analysis Reports: Document the current security status of the root and sub-accounts, as well as the risk points we

have identified based on the Security Settings Policy and our recommended solutions.



Security Analysis Report

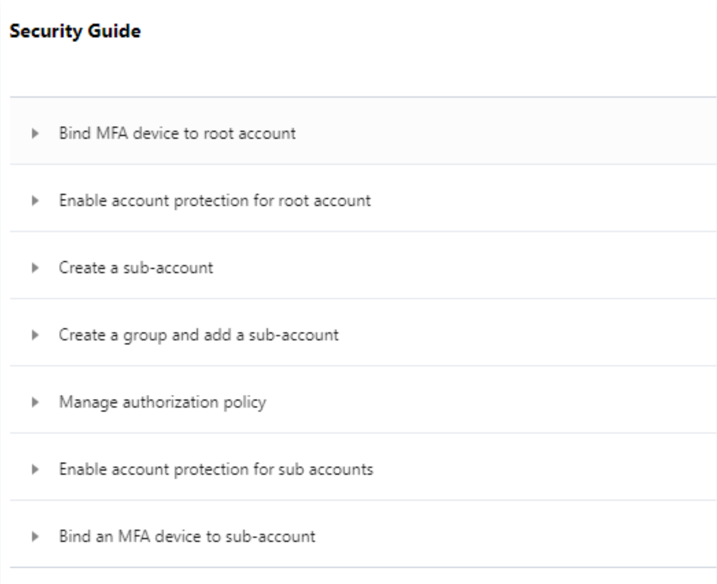
Click this button to download a report that lists the current security status of the Root account and sub-accounts, as well as the risk points we found and recommended solutions based on the Best Practices. A single report will be generated with a valid cache period of 4 hours.

Security Guide

> **Note**
> For the security of your accounts and assets in Tencent Cloud, we strongly recommend you complete all the configurations in the security guide.

The security guide module provides basic CAM feature descriptions and necessary security operation guidance, such as binding MFA devices to root accounts, enabling account protection for root accounts, creating sub-accounts, and creating groups and adding sub-accounts.

- Operational Permissions: Only the root account has the operational permissions for **Root Account MFA Device Binding** and **Root Account Protection Activation**. For the remaining five settings, all authorized users can perform operations.
- Guideline Status: Each guideline item is categorized into two states, **Unfinished** and **Completed**. The root account can view the status of each guideline item when logged into the console, while sub-accounts with permissions cannot view the status.
- Setting Entry: Sub-accounts with permissions can view the corresponding feature introductions and respective setting entries by clicking on the triangle symbol on the left of each guide item. The following image is an example of the Security Guidelines module after the root account logs into the console.



Security Guide

- Bind MFA device to root account
- Enable account protection for root account
- Create a sub-account
- Create a group and add a sub-account
- Manage authorization policy
- Enable account protection for sub accounts
- Bind an MFA device to sub-account

Users

Root account

Root Account Permissions

Last updated：2023-08-31 17:03:31

Scenario

This document describes how to configure root account permissions and message channels.

Preparations

You have registered a Tencent Cloud account, also known as the root account. For registration, please refer to Sign Up for Tencent Cloud.

Instructions

Root account does not require authorization

The root account inherently possesses all Tencent Cloud resources under the account and can access any of these resources without authorization. Therefore, it is not recommended to use the root account to manage resources. Instead, create sub-accounts and assign policies based on the principle of least privilege, using these limited-permission sub-accounts to manage your cloud resources. For more recommendations on account permissions, please refer to Security Best Practices.

Root account message channels

The security phone number and email address you provided when registering your Tencent Cloud root account will also serve as the initial message receiving channels. If you modify the security phone number or email address in the Account Center - Console, the contact phone number or email address used for Tencent Cloud message notifications in the Cloud Access Management (CAM) - Console will not be updated synchronously. To modify these, please refer to Root Account Message Subscription.

> ⚠ **Note**
> To prevent any loss due to missed messages, please promptly visit the Cloud Access Management (CAM) - Console to confirm whether the contact phone number or email address used for message subscription meets your expectations.

Associated Documents

- If you wish to learn how to modify the security mobile number or email address used for security verification of the root account, please refer to Frequently Asked Questions about Email and Mobile Number.
- If you wish to learn how to create a sub-user, please refer to Create a Sub-User.
- If you wish to understand how to set permissions for a sub-account, please refer to Authorization Management.

Root Account Message Subscription

Last updated：2023-08-31 17:04:14

Scenario

This document provides instructions on how to modify, verify message notification channels, and set up subscription messages for the primary account. If the primary account needs to receive message notifications, the primary account must verify the message channels. After subscribing to the messages, the primary account can receive relevant message alerts through the verified message channels.

Preparations

You have already logged into the Cloud Access Management Console and navigated to the User List Management Console page.

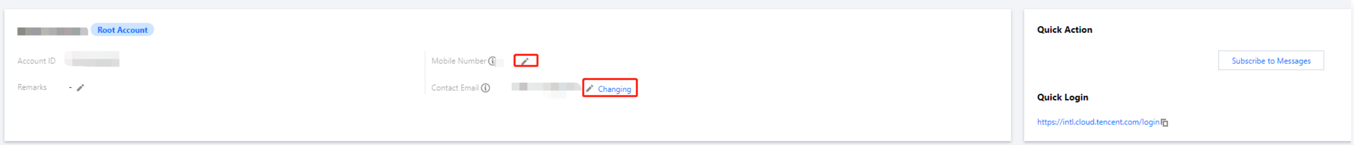
Instructions

Verifying message channels

1. Locate the root account from the user list.
2. Click on the username to enter the user details page.
3. On the user details page, click **Change in Progress** > **Resend Verification Link** under the user information bar. If there is no **Change in Progress** > **Resend Verification Link** button, it indicates that the message notification channel has been verified and no further action is required.
    - Contact Number: The system will send a verification message to the mobile number set for the primary account. Upon receiving the verification message, the user can confirm the link to complete the verification of the mobile message channel.
    - Contact Email: The system will send a verification message to the email address set by the primary account. Upon receiving the verification message, the user can confirm the link to complete the verification of the email message channel.
    - Contact WeChat: After completing email verification, the system will send an email containing a QR code to the primary account's set email. Scanning the code with WeChat and following the WeChat Official Account will complete the verification of the WeChat message channel.

Modifying message channels

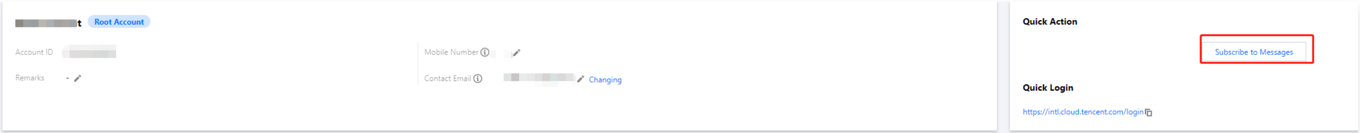
1. Locate the root account from the user list.
2. Click on the username to enter the user details page.
3. In the User Information module, click on the ✎ following the user information.



4. In the pop-up window for editing information, you can change the mobile phone, email, and WeChat information you need to modify.
5. To modify the message notification channel, you need to verify the message channel to receive messages normally. For verification instructions, please refer to Verify Message Notification Channel.

Setting message subscriptions

1. Locate the root account from the user list.
2. Click on the username to enter the user details page.
3. In the Quick Operations module, click **Subscribe to Messages**.



4. In the pop-up message subscription window, select the types of messages you wish to subscribe to (you can expand the list by clicking on the "►" button to select specific types of messages to receive).
5. Click **Confirm** to complete the subscription message configuration.

Associated Documents

If you want to know how to subscribe to messages for collaborators, please refer to Collaborator Message Subscription.
If you want to know how to subscribe to messages for sub-users, please refer to Sub-user Message Subscription.
If you want to know how to subscribe to messages for message recipients, please refer to Message Recipient Subscription.

Sub-Users

Creating Sub-User

Last updated：2023-08-31 17:35:48

Scenario

If you are a sub-account with admin permissions (AdministratorAccess) or full access to CAM (QcloudCamFullAccess) and have purchased CVM, VPC, COS, and other Tencent Cloud resources, you can create one or more sub-accounts for your team members and allow them to access your resources.
This document describes how to use the admin account to create a sub-user in the Cloud Access Management Console and bind the sub-user to a permission policy.

> **Note**
> Both sub-users and collaborators are sub-accounts. For definitions and permissions, please refer to User Types.

Creation method	Scenarios	Note
Quick Creation	Creating Admin User	By default, it has AdministratorAccess permissions, which can be modified.
Custom	Ordinary Sub-user	Bind policy permissions as needed
WeChat/WeCom Import	WeChat/WeCom Friends as Sub-Users	The Tencent Cloud account is already linked to WeChat/WeCom.

Preparations

You have already created a sub-account with admin permissions Create a sub-account with administrative privileges or a sub-account with full access to CAM (QcloudCamFullAccess).

Instructions

Creating a Role via Console

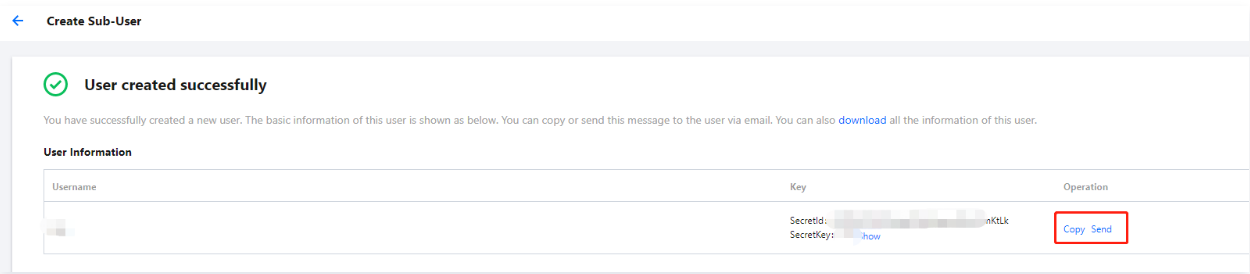
> **Note**
> - You can click the following tabs to view the directions to create and authorize different types of sub-accounts.
> - A root account with an unverified identity can create up to ten sub-accounts every 24 hours.

Quick Creation

1. Log in to the Tencent Cloud console, go to the User List, click **Create User** to access the Create User page.
2. On the Create User page, click **Quick Create** to navigate to the Quick Create User page.
3. On the quick user creation page, enter the username in **User Information** and adjust other options as needed.

   > **Note**
   > Click **Create User** to create up to 10 users at a time.

4. For "Password resetting required", select whether the sub-user needs to reset the password upon next login as needed.
5. Click **Create User** to navigate to the successful user creation page.
6. You can get the sub-user information in the following two methods:
   - Click **Send to** to supplement your email information, and the system will send the complete sub-user information to your email.
   - Click **Copy** and paste to save locally.



Create Sub-User

User created successfully

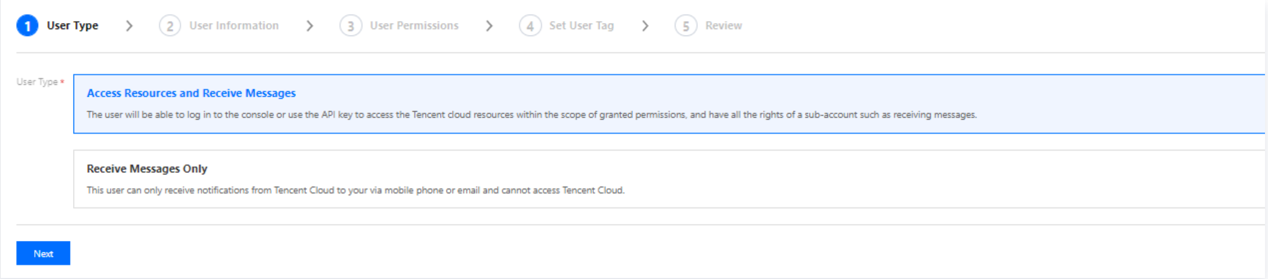
You have successfully created a new user. The basic information of this user is shown as below. You can copy or send this message to the user via email. You can also download all the information of this user.

User Information

Username	Key	Operation
[redacted]	SecretId: [redacted]nKtLk SecretKey: [redacted]how	Copy Send

Custom

1. Log in to the Cloud Access Management Console and select **Users** > User List from the left sidebar to access the user list management page.
2. On the User Management page, click **Create User** to navigate to the Create User page.
3. On the Create User page, click **Custom Create** to navigate to the Select User Type page.
4. On the Select User Type page, click **Access Resources and Receive messages** or **Receive messages Only**, then click **Next** to enter user information.



User Type *

Access Resources and Receive Messages

The user will be able to log in to the console or use the API key to access the Tencent cloud resources within the scope of granted permissions, and have all the rights of a sub-account such as receiving messages.

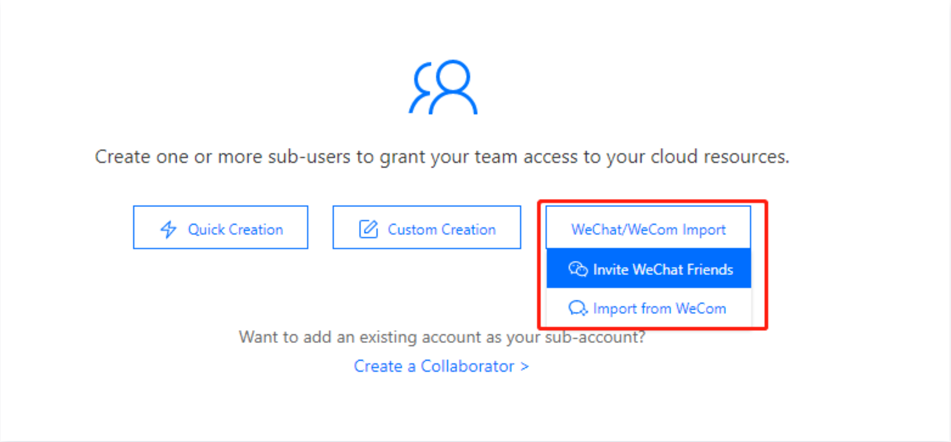
Receive Messages Only

This user can only receive notifications from Tencent Cloud to your via mobile phone or email and cannot access Tencent Cloud.

5. Follow the on-screen instructions to fill in and confirm the information, then click **Complete** to finish creating the custom sub-user.
   - If **Resource Access and Message Receipt** is enabled, you will be directed to the page indicating that the sub-user has been created successfully.
   - If it is for **receiving messages only**, navigate to the user list page.

WeChat/WeCom Import

1. Log in to the Tencent Cloud console, go to the User List, click **Create User** to access the Create User page.
2. On the Create User page, click **Import via WeChat/WeCom** and select **Invite via WeChat** or **Import via WeCom**.



Create one or more sub-users to grant your team access to your cloud resources.

Want to add an existing account as your sub-account?

Create a Collaborator >

3. Follow the on-screen instructions to complete the creation process. For detailed steps, refer to Creating Sub-users via WeChat or Importing Sub-users via WeCom.

Creating a role using API

You can add sub-users and set permissions by calling the AddUser API with an access key. For more information, see Add Sub-User - API Documentation.

> **Note:**
> When creating a sub-user via API, you can restrict the created sub-user to programmatic access only, as demonstrated below.

```
    {
  "statement": [
    {
      "action": [
        "cam:AddUser"
  ],
      "condition": {
        "for_any_value:bool_equal": {
          "cam:console_login": [
            "false"
      ]
}
      },
      "effect": "allow",
      "resource": [
        "*"
      ]
}
  ],
  "version": "2.0"
}
```

If you wish to understand how to manage sub-users by grouping and authorizing them through user groups, please refer to Adding/Removing Users from User Groups and Adding/Removing Policies from User Groups.
If you wish to learn how to add or delete associated policies for sub-users, please refer to Sub-User Permission Settings.
If you wish to understand how to log in as a sub-user, please refer to Sub-User Login.
If you wish to understand how to reset the key for a sub-user, please refer to Resetting the Login Password for Sub-Users.
If you wish to understand how to subscribe a sub-user to messages, please refer to Sub-User Message Subscription.

Importing Sub-Users via WeCom

Last updated：2023-08-31 21:42:34

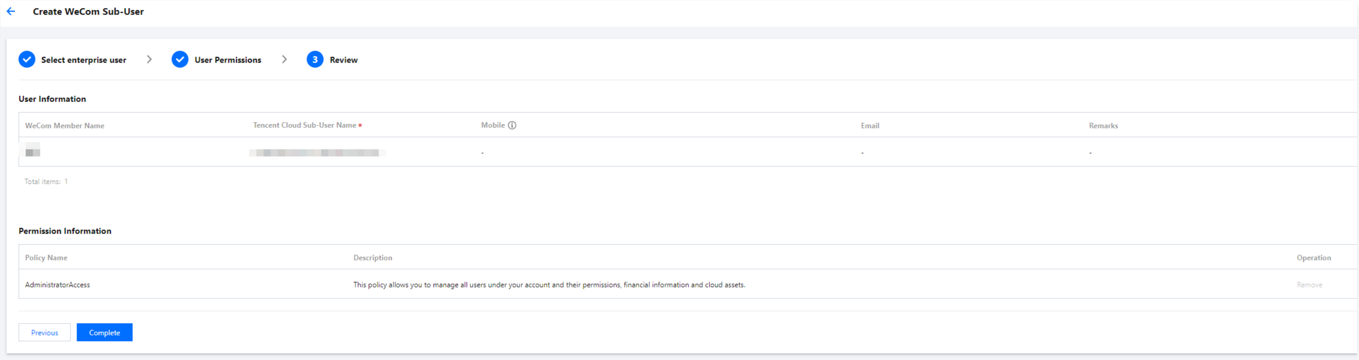
Scenario

This document provides guidance on how to import sub-users via WeCom and set permissions for these WeCom sub-users. The WeCom sub-users will manage resources under the primary account within the scope of their granted permissions.

Instructions

> **Note**
> - A root account with an unverified identity can create up to ten sub-accounts every 24 hours.
> - By default, WeCom sub-users are permitted to log in to the Tencent Cloud console. Currently, this permission cannot be revoked.
> - The WeCom sub-user login link can be obtained from **Cloud Access Management Console** > Overview > **Login Link** > **WeCom Sub-user**.

1. Log in to the Cloud Access Management Console, and in the left sidebar, click **Users** > User List to navigate to the user list management page.
2. On the User List Management page, click **Create User** to navigate to the Select User Type page.
3. On the **Select User Type** page, click **WeCom Import** under "WeChat/WeCom Import".
4. Select the **company name** that requires authorization, check the members who need to be authorized, and click **Next**.
5. After ensuring the user information is accurate, click **Next**.
6. Based on your actual needs, choose different methods to set permissions for the newly created WeCom sub-user. After associating the policy, the WeCom sub-user will obtain the permissions described in the policy. Once completed, click **Next**.
   - Acquiring group-associated permissions by adding to a group: Utilizing groups is the best practice for managing user permissions based on job functions. By associating permissions with a group, WeCom sub-users can be added to an existing user group or a newly created one. The WeCom sub-users can then be associated with the policies attached to that group.
   - Copy Existing User Policies: By copying the permissions of existing users, you can associate policies with sub-users. Click on **Copy Existing User Policies**, select the users whose policies you wish to copy, and the WeCom sub-users will be associated with the policies attached to the copied users.
   - To associate a policy from the policy list: Click **Associate a Policy from the Policy List** and select the policies you wish to associate.
7. After verifying the user and permissions, click **Complete** to finish importing sub-users via WeCom.



User Information

WeCom Member Name	Tencent Cloud Sub-User Name *	Mobile ⓘ	Email	Remarks
[redacted]	[redacted]	-	-	-

Total items: 1

Permission Information

Policy Name	Description	Operation
AdministratorAccess	This policy allows you to manage all users under your account and their permissions, financial information and cloud assets.	Remove

Associated Documents

If you wish to understand how to link a Tencent Cloud account with WeCom, please refer to Linking Tencent Cloud Account with WeCom.

If you wish to understand how to modify the scope of information that Tencent Cloud can obtain from the linked WeCom, please refer to Modifying WeCom Visibility Scope.

If you wish to understand how to manage sub-users by grouping them through user groups, please refer to User Management and User Group Permission Settings.
If you wish to understand how to add or remove associated policies for sub-users, please refer to Sub-user Permission Settings.
If you wish to understand how a sub-user can log in, please refer to Sub-user Login.
If you wish to understand how to subscribe to messages for sub-users, please refer to Sub-user Message Subscription.

Sub-user Security Credentials
Logging in as a sub-user

Last updated：2023-08-31 18:26:42

This document elucidates how to determine the type of your sub-account and log into it. Once logged in, the sub-account will manage the resources under the root account within its authorized scope.

Identifying Sub-account User Type

There are two methods to determine the type of your sub-account.

- Refer to the User Type documentation. You can determine the type of your sub-account based on the information provided in the document.
- Contact the root account or a sub-account with the cam:ListSubAccounts API permission to view the User Type column in the User List console.

Logging in to a Sub-account

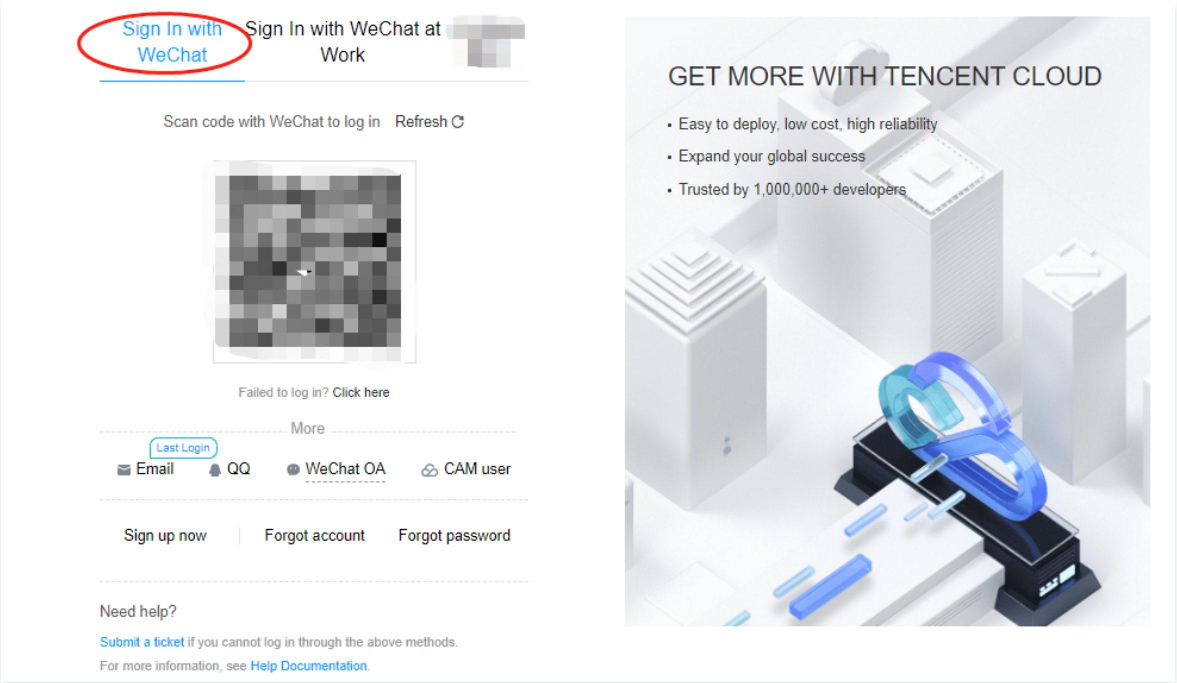
Collaborator Login

If your sub-account user type is a collaborator, you can use the login method associated with your root account to access the Tencent Cloud Account Login page and choose to log in as a collaborator. This allows you to manage the resources under the root account within your authorized scope. For more details, refer to Collaborator Login.

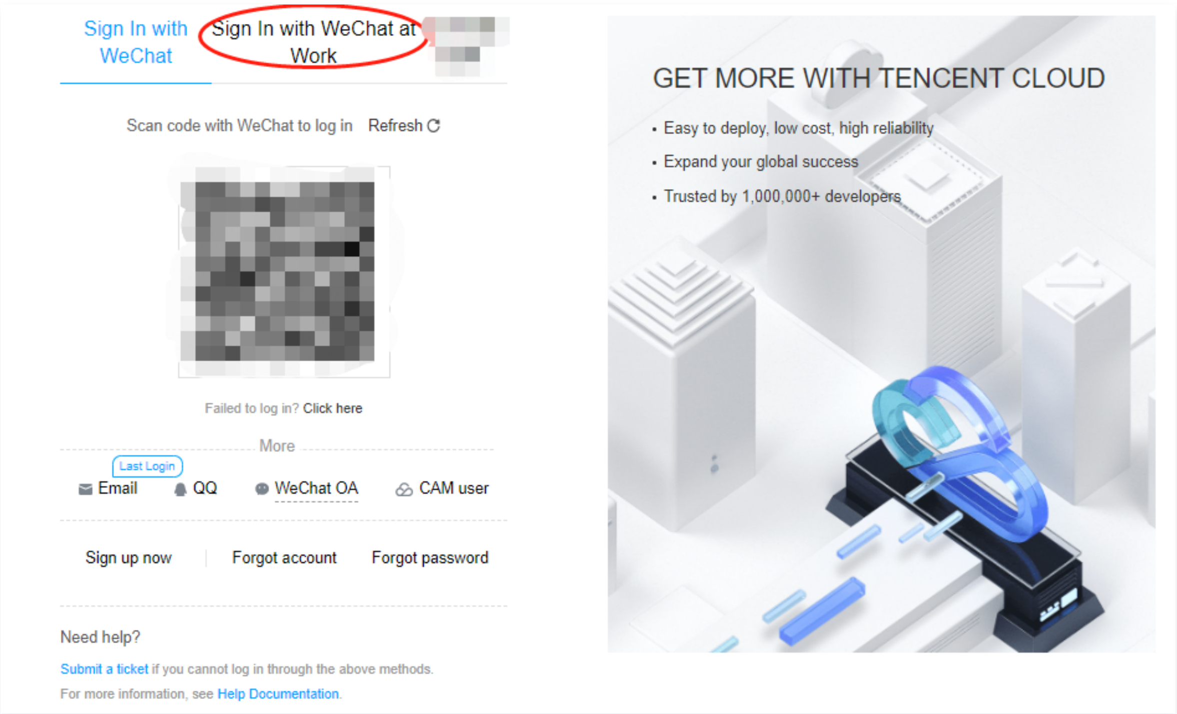
Logging in as a sub-user

There are several methods to log into your sub-account.

- If your sub-account user type is a sub-user, you can log into the sub-account by entering the root account ID, sub-user name, and login password on the Tencent Cloud Sub-user Login page. For more details, refer to Sub-user Login.
- If your sub-account type is a sub-user and you have completed the Sub-user Binding Login Method, you can go to the Tencent Cloud WeChat QR Code Login page, use the WeChat client's scan function to log into your account, and manage the resources under the root account within your authorized scope.


Sign In with WeChat
Sign In with WeChat at Work
Scan code with WeChat to log in
Refresh
Failed to log in? Click here
More
Last Login
Email
QQ
WeChat OA
CAM user
Sign up now
Forgot account
Forgot password
Need help?
Submit a ticket if you cannot log in through the above methods.
For more information, see Help Documentation.
GET MORE WITH TENCENT CLOUD
Easy to deploy, low cost, high reliability
Expand your global success
Trusted by 1,000,000+ developers

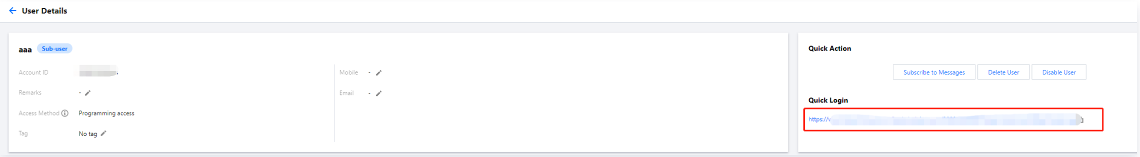
- If your sub-account type is a WeCom sub-user, you can navigate to the Tencent Cloud WeCom Sub-user Login page and use the scan function on your WeCom client to log into your sub-account.



Sign In with WeChat
Sign In with WeChat at Work
Scan code with WeChat to log in Refresh
Failed to log in? Click here
More
Last Login
Email
QQ
WeChat OA
CAM user
Sign up now
Forgot account
Forgot password
Need help?
Submit a ticket if you cannot log in through the above methods.
For more information, see Help Documentation.
GET MORE WITH TENCENT CLOUD
Easy to deploy, low cost, high reliability
Expand your global success
Trusted by 1,000,000+ developers

- You can also swiftly log in by switching from the root account to the sub-account.

1.1 On the **Users** > User List page, click the target **Username** to enter the **User Details** page, then click the link below Quick Login.



← User Details

aaa Sub-user

Account ID [redacted]

Remarks -

Access Method Programming access

Tag No tag

Mobile -

Email -

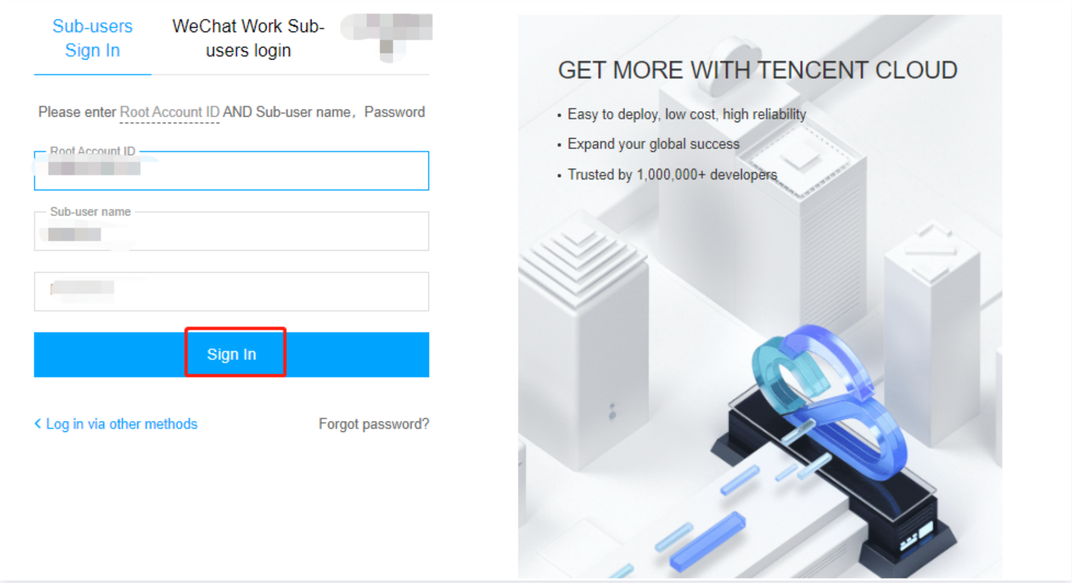
Quick Action

Subscribe to Messages | Delete User | Disable User

Quick Login

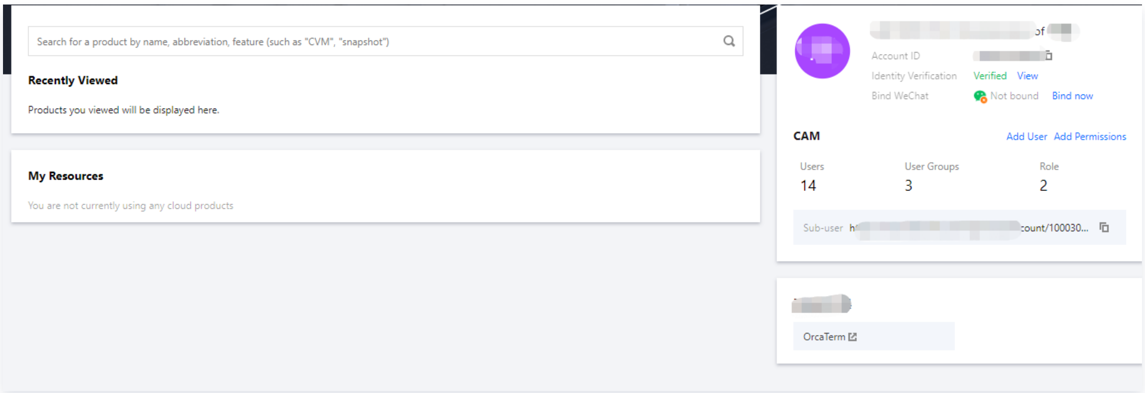
https://v[redacted]

1.2 On the **Login** page, enter the sub-account password and click **Sign in**.



Sub-users Sign In
WeChat Work Sub-users login
Please enter Root Account ID AND Sub-user name，Password
Root Account ID
Sub-user name
Sign In
Log in via other methods
Forgot password?
GET MORE WITH TENCENT CLOUD
Easy to deploy, low cost, high reliability
Expand your global success
Trusted by 1,000,000+ developers

1.3 Upon successful login, you will be automatically redirected to the sub-account page.



Search for a product by name, abbreviation, feature (such as "CVM", "snapshot")

Recently Viewed

Products you viewed will be displayed here.

My Resources

You are not currently using any cloud products

[redacted] of [redacted]

Account ID	[redacted]
Identity Verification	Verified View
Bind WeChat	Not bound Bind now

CAM Add User Add Permissions

Users	User Groups	Role
14	3	2

Sub-user h[redacted]count/100030...

[redacted]

OrcaTerm

Resetting Login Passwords for Sub-Users

Last updated：2023-08-31 18:28:19

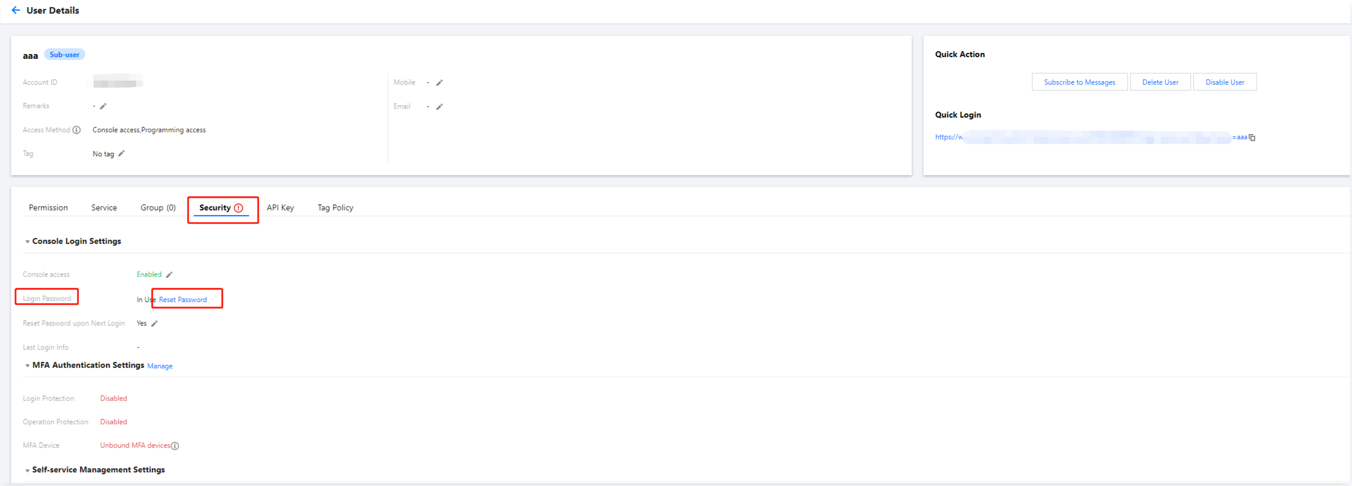
Scenario

This document describes how to modify the passwords of sub-users. After modification, the sub-user can use the new password to log in and manage resources under the root account.

Instructions

> **Note**
> This procedure is only applicable to sub-users created through custom and WeChat invitation methods. Sub-users imported through WeCom currently only support login management via WeCom QR code scanning.

1. In the User List, select the sub-user whose password needs to be changed, select the specific **User Name**, and enter the user details page.
2. In the User Details page, select **Security** > **Console Login Settings** > **Login Password**, and click **Reset Password**. As shown in the figure below:



User Details

aaa Sub-user

Account ID [redacted]

Remarks -

Access Method Console access,Programming access

Tag No tag

Mobile -

Email -

Quick Action

Quick Login

https://w[redacted]=aaa

Console Login Settings

Console access Enabled

Login Password In Use Reset Password

Reset Password upon Next Login Yes

Last Login Info -

MFA Authentication Settings Manage

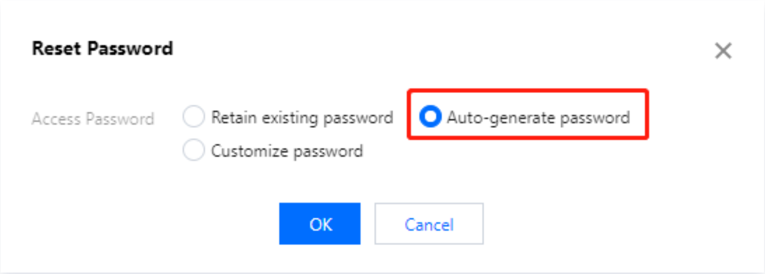
Login Protection Disabled

Operation Protection Disabled

MFA Device Unbound MFA devices

Self-service Management Settings

3. In the pop-up **Reset Password** window, set the current user's password as shown below:



Reset Password

Access Password ○ Retain existing password ● Auto-generate password ○ Customize password

If you need to set a new password for the sub-user, you can do so in one of the following two ways.

- If you select **Auto-generate password** in the **Access Password** section, the system will automatically generate a console login password. You can copy and save this password, and if necessary, click **Download .csv** to save the password.
- If you select **Customize password** in **Access Password**, enter the console login password you have set for this sub-user.
  - If you require the current user to reset their password independently, you can select **Need to reset password**. The sub-user will be prompted to reset their console login password after their next successful login.

Associated Documents

If you wish to learn how to create sub-users through a custom method, please refer to Creating Sub-Users Custom.
If you wish to learn how to create sub-users through WeChat invitation, please refer to Creating Sub-Users via WeChat.
If you wish to learn how to modify the collaborator's login password, please refer to Changing Account Password.

Setting the Sub-User Login Method

Last updated：2023-08-31 16:56:11

Scenario

This document outlines the process of binding and unbinding the WeCom login method for sub-users (only supports sub-users created through customization and WeCom).

Preparations

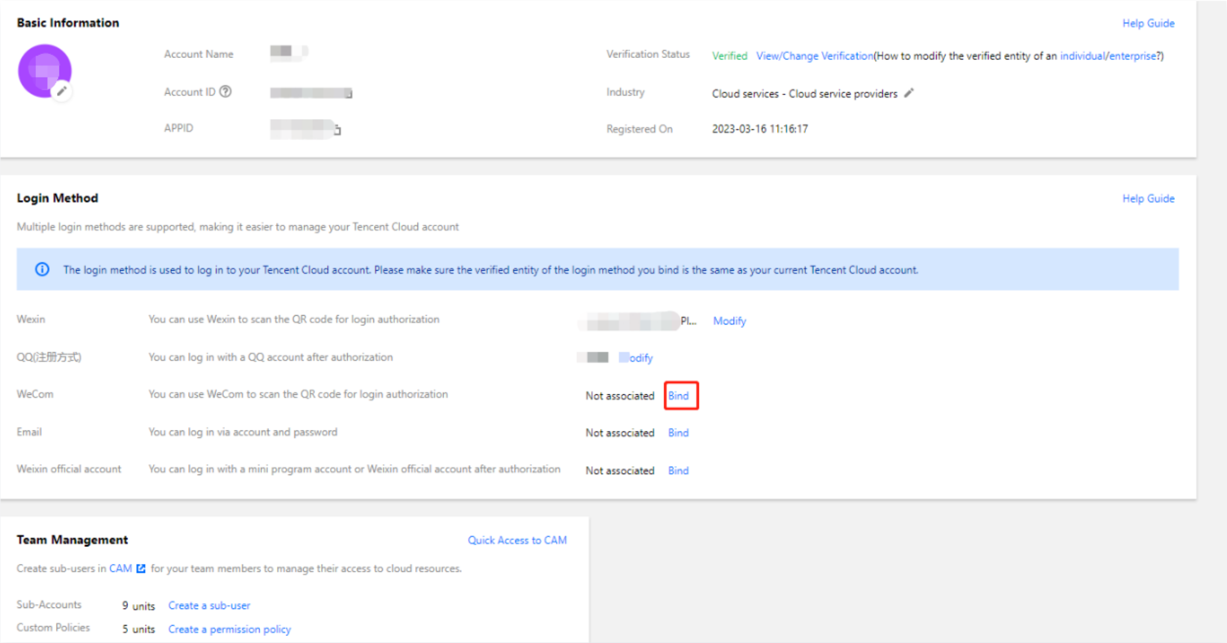
You have logged in as the sub-user that needs to be set (only supports sub-users created through customization or WeCom), and navigated to the Account Information - Console page.

Instructions

Binding the login method for sub-users

Follow the steps below to bind the WeCom login method for your sub-users. Once successfully bound, you can log in to the sub-user via WeCom QR code scanning and manage resources under the root account within the scope of permissions.

1. On the Account Information management page, click **Bind** under the login method column.



Basic Information Help Guide

Account Name	[redacted]	Verification Status	Verified View/Change Verification(How to modify the verified entity of an individual/enterprise?)
Account ID	[redacted]	Industry	Cloud services - Cloud service providers
APPID	[redacted]	Registered On	2023-03-16 11:16:17

Login Method Help Guide

Multiple login methods are supported, making it easier to manage your Tencent Cloud account

ⓘ The login method is used to log in to your Tencent Cloud account. Please make sure the verified entity of the login method you bind is the same as your current Tencent Cloud account.

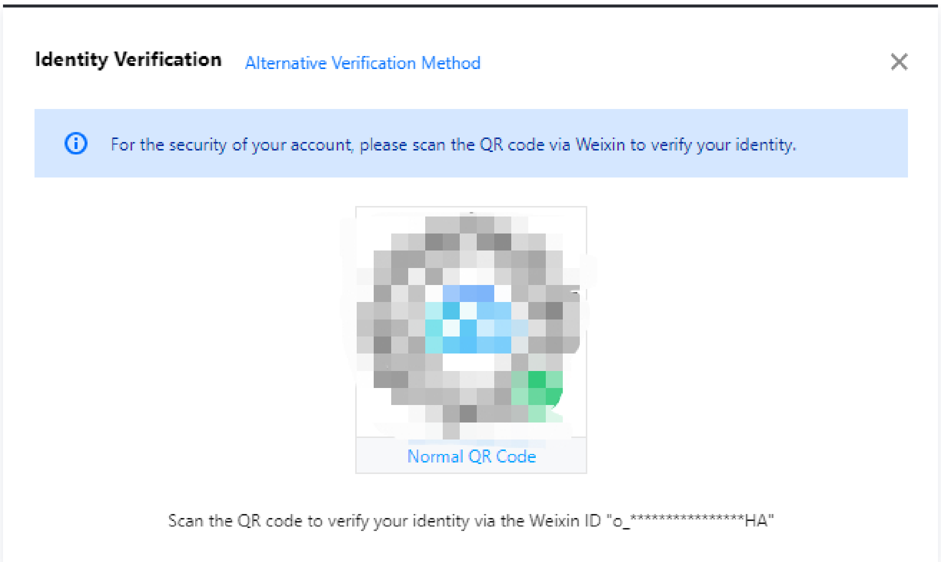
Wexin	You can use Wexin to scan the QR code for login authorization	[redacted] Pl...	Modify
QQ(注册方式)	You can log in with a QQ account after authorization	[redacted]	odify
WeCom	You can use WeCom to scan the QR code for login authorization	Not associated	Bind
Email	You can log in via account and password	Not associated	Bind
Weixin official account	You can log in with a mini program account or Weixin official account after authorization	Not associated	Bind

Team Management Quick Access to CAM

Create sub-users in CAM for your team members to manage their access to cloud resources.

Sub-Accounts	9 units	Create a sub-user
Custom Policies	5 units	Create a permission policy

2. Complete the identity verification on the pop-up **Identity Verification** page.



Identity Verification Alternative Verification Method

For the security of your account, please scan the QR code via Weixin to verify your identity.

Normal QR Code

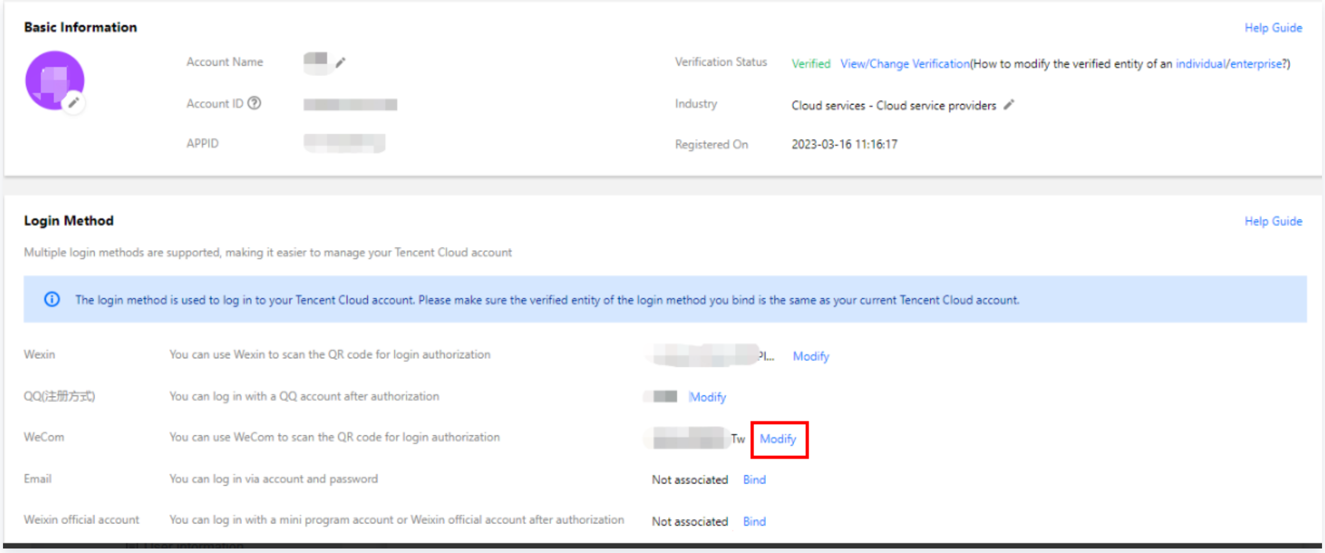
Scan the QR code to verify your identity via the Weixin ID "o_****************HA"

3. In the pop-up **Scan to Bind WeCom** window, use the scan function of the WeCom client to scan the QR code on the page.
4. Your WeCom client will receive a Tencent Cloud login confirmation prompt. Click **Allow** to complete the operation of binding the login method for the sub-user.

Modifying or Unbinding the Login Method for Sub-Users

Follow the steps below to unbind the WeCom login method for your sub-users. After successful unbinding, you will not be able to log in to your sub-user account using the WeCom QR code scan.

1. On the Account Information management page, click **Modify** under the Login Method section.



Basic Information Help Guide

Account Name	[redacted]	Verification Status	Verified View/Change Verification(How to modify the verified entity of an individual/enterprise?)
Account ID	[redacted]	Industry	Cloud services - Cloud service providers
APPID	[redacted]	Registered On	2023-03-16 11:16:17

Login Method Help Guide

Multiple login methods are supported, making it easier to manage your Tencent Cloud account

The login method is used to log in to your Tencent Cloud account. Please make sure the verified entity of the login method you bind is the same as your current Tencent Cloud account.

Wexin	You can use Wexin to scan the QR code for login authorization	[redacted]PI...	Modify
QQ(注册方式)	You can log in with a QQ account after authorization	[redacted]	Modify
WeCom	You can use WeCom to scan the QR code for login authorization	[redacted] Tw	Modify
Email	You can log in via account and password	Not associated	Bind
Weixin official account	You can log in with a mini program account or Weixin official account after authorization	Not associated	Bind

2. Complete the identity verification on the pop-up **Identity Verification** page.
3. Select the operation you wish to perform, and use the Scan function of the WeCom client to scan the QR code on the page.
4. Your WeCom client will receive an operation confirmation alert. Click **Confirm** to complete the unbinding of the sub-user's login method.

Associated Documents

If you wish to learn how to create a sub-user through customization or WeChat, please refer to Custom Creation of Sub-Users and Creating Sub-Users via WeChat.

If you wish to learn how to log in as a sub-user, please refer to Sub-User Login.

Setting security protection for sub-users

Last updated：2023-08-31 18:31:29

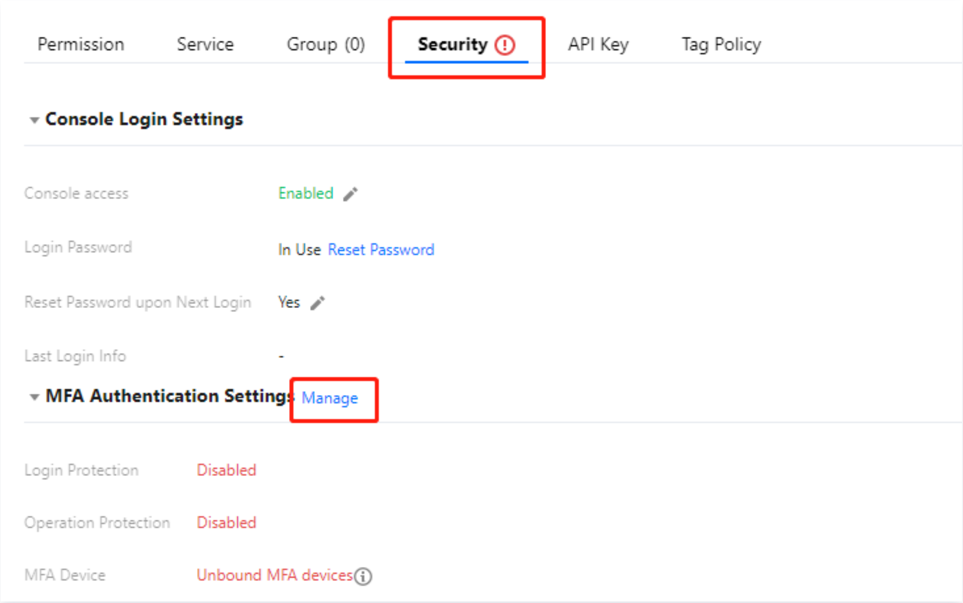
Scenario

This document describes how to enable and disable security protection for sub-users. This will determine if sub-users need to go through security verification.

Instructions

Enabling security protection for sub-users

1. Log in to the Cloud Access Management Console and select **Users** > **User List** from the left sidebar to navigate to the user list management page.
2. On the user list management page, locate the sub-user for whom you want to set up security protection.
3. Click on the **username** to access the user's detailed information page.
4. On the user details page, click **Security** to navigate to the security management page.
5. On the Security Management page, click **Manage** next to **MFA Authentication Settings**. As shown in the image below:



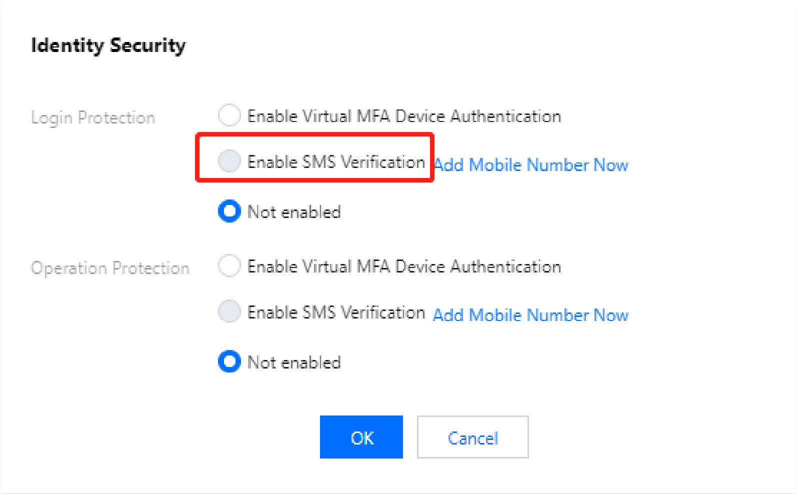
Console Login Settings

Console access	Enabled
Login Password	In Use Reset Password
Reset Password upon Next Login	Yes
Last Login Info	-

MFA Authentication Settings Manage

Login Protection	Disabled
Operation Protection	Disabled
MFA Device	Unbound MFA devices

6. In the Identity Security pop-up window, select the type of protection you wish to enable, and activate the corresponding security protection for the current sub-user.



Identity Security

Login Protection
○ Enable Virtual MFA Device Authentication
○ Enable SMS Verification Add Mobile Number Now
● Not enabled

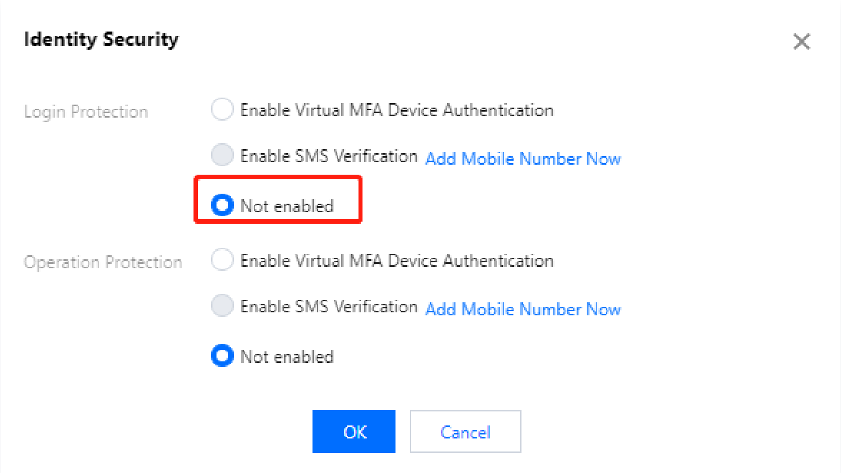
Operation Protection
○ Enable Virtual MFA Device Authentication
○ Enable SMS Verification Add Mobile Number Now
● Not enabled

7. Click **OK** to finalize the process of enabling security protection for sub-users.

Note
Upon enabling virtual MFA device verification, the sub-user is required to bind the MFA device at their next login, following the instructions provided on the page.

Disabling security protection for sub-users

1. Follow the steps 1 – 5 in Enabling Security Protection to access the Identity Security window.
2. In the Identity Security pop-up window, set the protection type you wish to disable to **Not enabled**.



Identity Security

Login Protection
○ Enable Virtual MFA Device Authentication
○ Enable SMS Verification Add Mobile Number Now
● Not enabled

Operation Protection
○ Enable Virtual MFA Device Authentication
○ Enable SMS Verification Add Mobile Number Now
● Not enabled

3. Click **OK** to complete the process of disabling security protection for the sub-user.

Sub-user Message Subscriptions

Last updated：2023-08-31 18:32:03

Scenario

This document provides guidance on how to verify message channels for sub-users and set up message subscriptions. If a sub-user needs to receive messages, they must first verify their message channels. Once the message channels are verified and messages are subscribed to, the sub-user can receive relevant message notifications through their verified channels.

Operations Guide

Verifying message channel

1. Log in to the Cloud Access Management Console and navigate to the User List management page.
2. Locate the sub-user to set the message subscription for.
3. Click on the **User Nickname** to access the user details page.
4. On the user details page, click **Replace - Resend Verification Link** under the user information bar.
   - Mobile: The system will send a verification message to the mobile number set by the sub-user. Once the user receives the verification message and confirms the link, the mobile message channel verification is completed.
   - Email: The system will send a verification message to the email address set for the sub-user. The user can complete the email message channel verification by confirming the link in the verification message.
   - Allowing WeChat to receive notifications: After completing email verification, the system will send an email containing a QR code to the sub-user's designated email address. Scanning the QR code and following the WeChat Official Account will complete the verification of the WeChat message channel.

> **Note**
>
> If your sub-user is currently not associated with any message channels, you can click on ✎ to supplement the information, then click on **Confirm**. The corresponding message channel will receive a verification message. Follow the above guidelines to complete the verification.

Setting message subscriptions

1. Log in to the Cloud Access Management Console and navigate to the User List management page.
2. Locate the sub-user to set the message subscription for.
3. Click on the **User Nickname** to access the user details page.
4. On the user details page, click **Subscribe to Messages** in the quick operations bar on the right.
5. A **Subscribe to Messages** window will pop up. You can select the message types here. Click ▼ to expand for granular selection options.
6. Click **OK** to finalize the subscription message configuration.

Querying Sub-User Information

Last updated：2023-08-31 16:57:52

Scenario

This document describes how to view user information, such as message subscriptions, notes, last login time, last login method, MFA device status, and how to search for sub-users by using keywords such as username, account ID, SecretId, mobile number, email, and notes.

Preparations

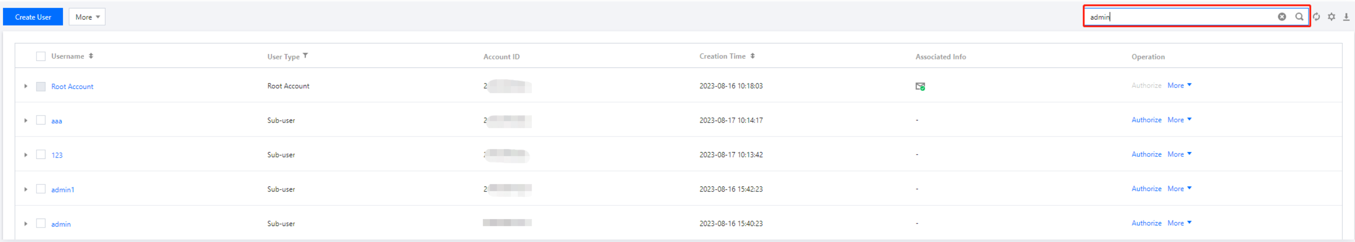
You have logged into the Cloud Access Management Console and navigated to the User List management page.

Instructions

Searching for Sub-users Using the Search Box

When there are numerous sub-users, you can search for them using keywords such as username, account ID, SecretId, mobile number, email, and notes.

1. On the User List management page, locate the search box in the upper right corner.
2. Enter the keyword in the search box and click on the search icon on the right. This will display the relevant sub-users, completing the operation of finding sub-users through the search box.



Username	User Type	Account ID	Creation Time	Associated Info	Operation
Root Account	Root Account	2[redacted]	2023-08-16 10:18:03	✉	Authorize More ▾
aaa	Sub-user	2[redacted]	2023-08-17 10:14:17	-	Authorize More ▾
123	Sub-user	[redacted]	2023-08-17 10:13:42	-	Authorize More ▾
admin1	Sub-user	2[redacted]	2023-08-16 15:42:23	-	Authorize More ▾
admin	Sub-user	[redacted]	2023-08-16 15:40:23	-	Authorize More ▾

View Sub-user Information

Viewing sub-user information in the expanded drawer

You can expand to view sub-user information, which includes user groups, message subscriptions, login protection, operation protection, MFA device status, and console access status.

1. On the User List management page, locate the sub-user you wish to view.
2. Click on the "▶" icon in the details column on the left.
3. In the expanded drawer, you can view the relevant information of the sub-user, thus completing the operation of viewing sub-user information through the drawer.

Viewing Sub-user Information via User Details

On the user details page, you can view detailed information about the sub-user, including basic information, quick operations and quick login entries, permissions, and services.

1. On the User List management page, locate the sub-user you wish to view.
2. Click on the username to enter the user details page.
3. On the User Details page, view the detailed information of the sub-user.

Deleting Sub-Users

Last updated：2023-08-31 16:59:25

Scenario

This document describes how to delete one or multiple sub-users. After deletion, the sub-users will no longer have root account management permissions.

Preparations

You have logged into the Cloud Access Management Console and navigated to the User List management page.

Instructions

Delete a single sub-user

1. On the User List management page, locate the sub-user(s) you wish to delete.
2. Click on **More** > **Delete** in the operation column on the right.
3. In the pop-up window for deleting users, ensure that the API keys under the current sub-user have been disabled and deleted. For more details, please refer to Access Keys.
4. Click **Confirm Deletion** to complete the removal of a single sub-user.

Delete multiple sub-users

1. In the User List management page, select the users that you want to delete by checking the checkbox on the left.
2. Click on **More Actions** at the top left, then select **Delete**.
3. In the pop-up window for deleting users, ensure that the API keys under the sub-users have been disabled and deleted. For more details, please refer to Access Keys.
4. Click **Confirm Deletion** to complete the removal of multiple sub-users.

Collaborators
Creating Collaborator

Last updated：2023-08-31 18:35:22

Scenario

If you are an admin user and have purchased CVM, VPC, COS, and other Tencent Cloud resources, you can set the Tencent Cloud accounts of other members of your team as collaborators and allow them to access your resources.
This document describes how to use the admin account to create a collaborator in the Cloud Access Management Console and bind the collaborator to a permission policy.

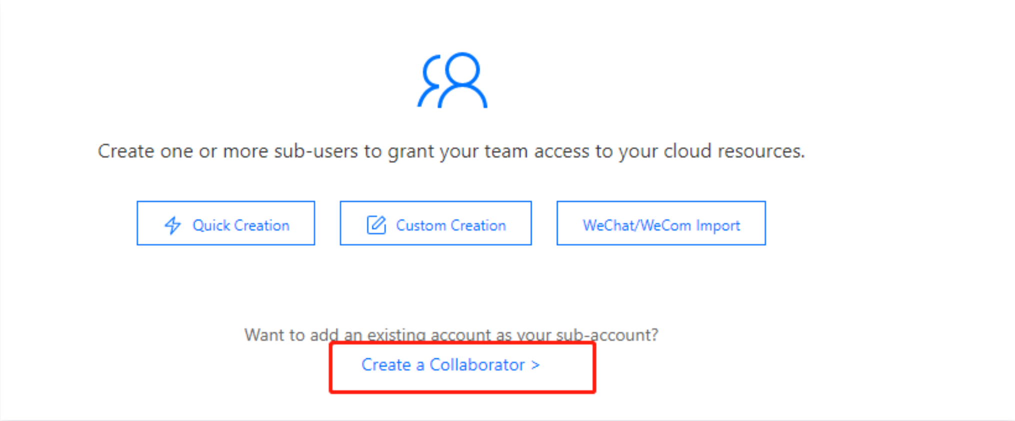
> **Note**
> Both collaborators and sub-users are sub-accounts. For definitions and permission descriptions, please refer to User Types.

Preparations

- You have created an admin user. For more information, see Create an Admin User.
- You already have a Tencent Cloud account that can be set as a collaborator (if not, please register a Tencent Cloud account first).

Operations Guide

1. Log in to the Tencent Cloud console, go to the User List, click **Create User** to access the Create User page.
2. On the Create User page, click **Create a Collaborator**.


Create one or more sub-users to grant your team access to your cloud resources.
Quick Creation
Custom Creation
WeChat/WeCom Import
Want to add an existing account as your sub-account?
Create a Collaborator >

3. Enter the relevant user information and click **Next**.

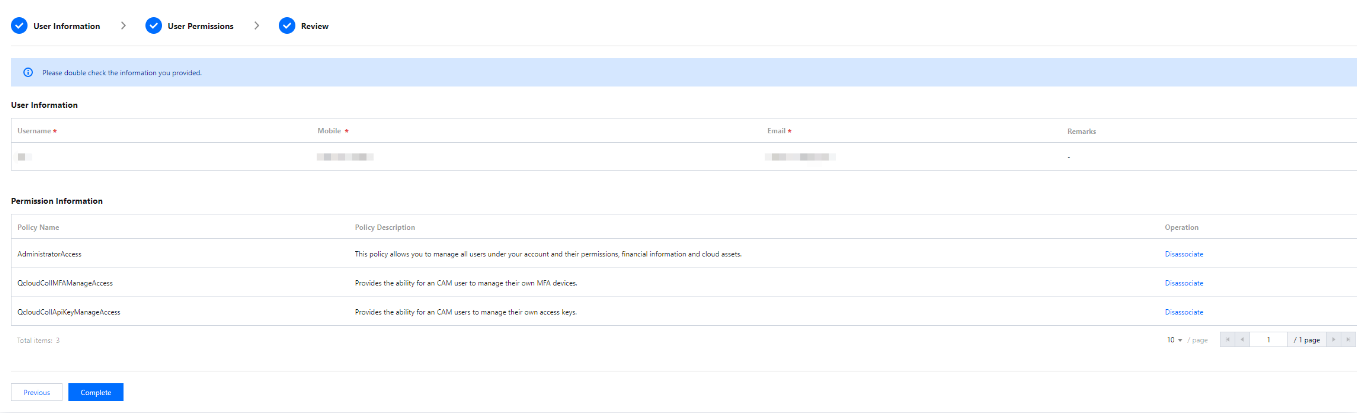
> **Note**
> - By default, collaborators are allowed to log in to the Tencent Cloud console. You can disable console access in the **Security** > **Console Login Settings** on the user details page.
> - To ensure the security of your account, it is recommended that you enable login and operation protection.
> - The account ID is a unique identifier in Tencent Cloud. The collaborator you are about to add needs to check it in Account Center - Account Information.

4. To set permissions, you can use one of the following three methods to set permissions for the newly created collaborator. The policy describes the permissions, and the collaborator obtains the permissions described in the policy after the policy is associated.
   - Add to group to obtain group permissions: Using groups is the best practice for managing user permissions based on job functions. You can obtain permissions through group association. Click **Add to group to obtain group permissions**, select the

required user group, add the collaborator to an existing or newly created user group, and the collaborator can be associated with the policy attached to the group.

  - Copy Existing User Policy: To associate a collaborator with a policy by copying the permissions of an existing user, click **Copy Existing User Policy**, select the user whose policy you want to copy, and the collaborator will be associated with the policy attached to the copied user.
  - To authorize from the policy list, click **Select Policies to Associate from the Policy List** and select the policies you need to associate.

5. Click **Complete** to finish creating a new collaborator.



Please double check the information you provided.

User Information

Username *	Mobile *	Email *	Remarks
[redacted]	[redacted]	[redacted]	-

Permission Information

Policy Name	Policy Description	Operation
AdministratorAccess	This policy allows you to manage all users under your account and their permissions, financial information and cloud assets.	Disassociate
QcloudCollMFAManageAccess	Provides the ability for an CAM user to manage their own MFA devices.	Disassociate
QcloudCollApiKeyManageAccess	Provides the ability for an CAM users to manage their own access keys.	Disassociate

Total items: 3

Associated Documents

If you want to know how the newly created collaborator account logs into Tencent Cloud, please refer to Sub-account Console Login - Collaborator Login.

Setting Collaborator Permissions

Last updated：2023-08-31 18:36:03

Scenario

This document describes how to associate/disassociate a policy with/from a collaborator. The collaborator can manage the resources under the root account within the scope of the granted permissions.

Operations Guide

Associating a policy with a collaborator

Direct Association

You can directly associate a policy with a user to give them the permissions included in the policy.

1. Log in to the Tencent Cloud console, navigate to the User List, locate the collaborator to whom you wish to grant policy, and click **Authorize** in the operation column on the right.
2. Select the policy or policies to be authorized (multiple selections are allowed), then click **OK** to complete the process of associating the policy with the collaborator.

Association with Group

You can add a user to a user group, and the user will automatically obtain the permissions of the policy associated with that group. The type of policy obtained in this way is associated with the group. To remove a group-associated policy, the user must be removed from the corresponding user group.

1. Log in to the Tencent Cloud console, navigate to the User List, locate the collaborator to whom you wish to grant policy, and click on **More Actions** > **Add to Group** in the operation column on the right.
2. Select the user groups (multiple selections allowed) to which you want to add, then click **Confirm** to complete the operation of associating the policy with the group.

Disassociating a collaborator from a policy

Direct disassociation

You can directly disassociate a user from a policy to remove the permissions granted.

1. Log in to the Tencent Cloud console, navigate to the User List, locate the collaborator whose policy association needs to be disassociated, click on the collaborator's **User Name**, and enter the collaborator's details page.
2. Click **Permissions**, locate the policy to be disassociated in the list, and then click **Disassociate** in the operation column on the right.
3. Click **Confirm Disassociation** to complete the disassociation of the policy from the collaborator. After disassociation, the user will no longer have the permissions described in the policy.

Removing a collaborator from a group

You can remove a collaborator from a user group to automatically disassociate the user from the permissions associated with the group.

1. Log in to the Tencent Cloud console, navigate to the User List, locate the collaborator from whom you wish to disassociate the policy, and click on the collaborator's name to access their details.
2. Click on **Group**, find the group that needs to be removed from the list, and click **Remove from this Group** in the operation column on the right.
3. Click **Confirm** to remove the collaborator from the user group, thereby disassociating the group-related policy. After removal, the collaborator will no longer have access to the permissions associated with this group.

Collaborator Security Credentials

Collaborator Login

Last updated：2023-08-31 18:36:36

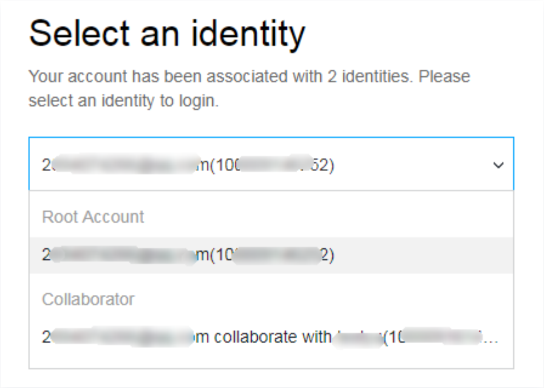
Scenario

This document describes how to log in to a collaborator’ s account. After logging in, the collaborator can manage the resources under the root account within the scope of permissions.

Instructions

> **Note**
> A collaborator account has two identities: its own root account identity and the identity of a collaborator for another account. Logging in as a collaborator does not require additional account passwords. After you log in with your regular account, you will enter the identity selection page. Simply select the identity you wish to log in with.

1. Navigate to the Tencent Cloud Account Login page to log in to your account. Please use the login method associated with your root account identity.
2. On the select an identity page, you can choose the user identity you wish to log in with. If your login account has a collaborator identity, you can choose to log in as a collaborator. For example, when logging in with QQ, the interface is as follows:



Select an identity

Your account has been associated with 2 identities. Please select an identity to login.

2[redacted]m(10[redacted]52)

Root Account

2[redacted]m(10[redacted]2)

Collaborator

2[redacted]m collaborate with [redacted](1[redacted]...

3. After selecting the desired identity from the dropdown box, click **Log in** to complete the collaborator login process.

Setting security protection for collaborators

Last updated：2023-08-31 18:37:29

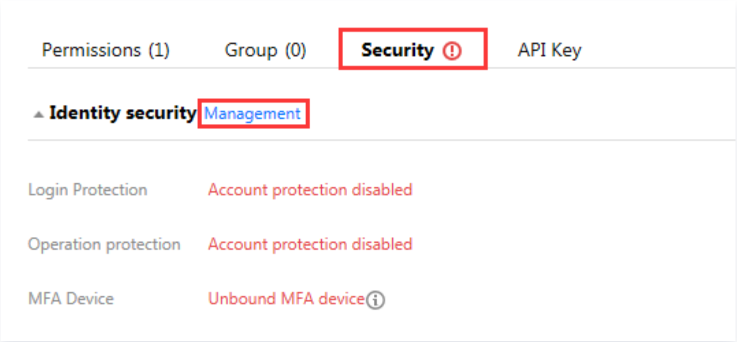
Scenario

This document describes how to enable and disable security protection for collaborators. This will determine if collaborators need to go through security verification.

Instructions

Enabling security protection for collaborators

1. Log in to the Cloud Access Management Console and select **Users** > User List from the left sidebar to navigate to the user list management page.
2. On the User List management page, select the collaborator for whom to configure security protection.
3. Click on the **username** to access the user's detailed information page.
4. On the user details page, click **Security** to navigate to the security management page.
5. On the security management page, click **Management** next to **Identity security**, as shown below:



Login Protection: Account protection disabled

Operation protection: Account protection disabled

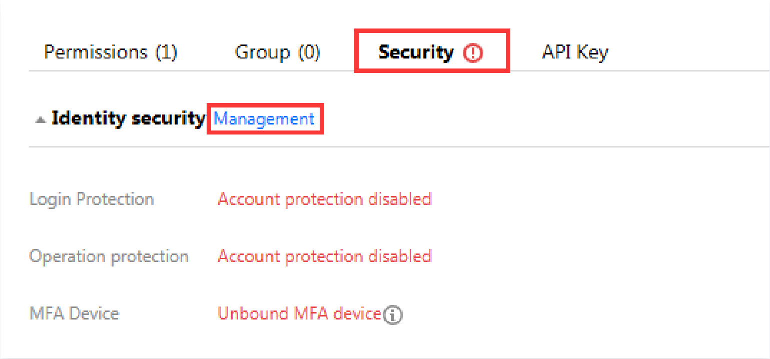
MFA Device: Unbound MFA device

6. In the **Identity security** window that pops up, select the protection type you want to enable for the collaborator.
7. Click **OK** to finalize the process of enabling security protection for collaborators.

> **Note**
> If virtual MFA device verification is enabled, the collaborator will need to bind the MFA device as prompted the next time they log in.

Disabling security protection for collaborators

1. Log in to the Cloud Access Management Console and select **Users** > User List from the left sidebar to navigate to the user list management page.
2. On the User List management page, select the collaborator for whom to configure security protection.
3. Click on the **username** to access the user's detailed information page.
4. On the user details page, click **Security** to navigate to the security management page.
5. On the security management page, click **Management** next to **Identity security**, as shown below:



Login Protection Account protection disabled

Operation protection Account protection disabled

MFA Device Unbound MFA device

6. In the **Identity security** window that pops up, select the protection type you want to disable for the collaborator.
7. Click **OK** to complete the process of disabling security protection for collaborators.

Collaborator Message Subscriptions

Last updated：2023-08-31 18:37:54

Scenario

This document provides guidance on how to verify message channels for collaborators and set up subscription messages. If a collaborator needs to receive messages, they must verify the message channels. Once the messages are subscribed for them, the user can receive relevant message alerts through the verified message channels.

Instructions

Verifying message channel

1. Log in to the Cloud Access Management Console and select **Users** > User List from the left sidebar to navigate to the user list management page.
2. On the User List Management page, locate the collaborator who needs to subscribe to messages.
3. Click on the **User Nickname** to access the user details page.
4. On the user details page, click **Replace - Resend Verification Link** under the user information bar.
   - Mobile: The system will send a verification message to the collaborator's set mobile number. The user can complete the mobile message channel verification by confirming the link received in the verification message.
   - Email: The system will send a verification message to the collaborator's set email address. The user can complete the email message channel verification by confirming the link received in the verification message.
   - Allow WeChat to receive notifications: After completing email verification, the system will send an email containing a QR code to the collaborator's set email. Scanning the QR code with WeChat and following the WeChat Official Account will complete the verification of the WeChat message channel.

> **Note**
>
> If your sub-user is currently not associated with any message channels, you can click on ✎ to supplement the information, then click **Confirm**. The corresponding message channel will receive a verification message. Follow the above guidelines to complete the verification.

Setting message subscriptions

1. Log in to the Cloud Access Management Console and select **Users** > User List from the left sidebar to navigate to the user list management page.
2. On the User List Management page, locate the collaborator who needs to subscribe to messages.
3. Click on the **User Nickname** to access the user details page.
4. On the user details page, click **Subscribe to Messages** in the quick operations bar on the right.
5. A **Subscribe to Messages** window will pop up. You can select the message types here. Click ▼ to expand for granular selection options.
6. Click **OK** to finalize the subscription message configuration.

Querying Collaborator Information

Last updated：2023-08-31 18:38:30

Scenario

This document provides guidance on how to view information such as the collaborator's user group, message subscription, login protection, operation protection, MFA device status, and console access status. It also explains how to search for collaborators using keywords such as username, account ID, SecretId, mobile number, email, and notes.

Preparations

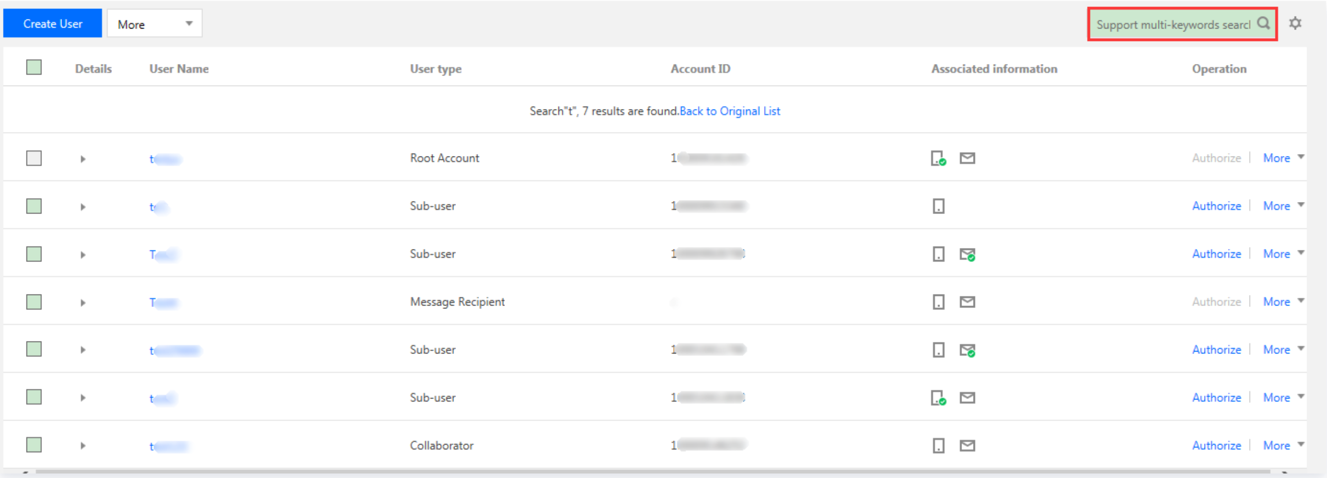
You have logged into the Cloud Access Management Console and navigated to the User List management page.

Instructions

Search for collaborators using search box

When there are numerous sub-users, you can search for collaborators using keywords such as username, account ID, SecretId, mobile number, email, and notes.

1. On the User List management page, locate the search box in the upper right corner.
2. Enter the keyword in the search box and click on the search icon on the right. This will display the relevant collaborators, completing the process of finding collaborators through the search box.



Search"t", 7 results are found.Back to Original List

☐	Details	User Name	User type	Account ID	Associated information	Operation
☐	▸	t[redacted]	Root Account	1[redacted]	📱 ✉	Authorize | More ▾
☐	▸	t[redacted]	Sub-user	1[redacted]	📱	Authorize | More ▾
☐	▸	T[redacted]	Sub-user	1[redacted]	📱 ✉	Authorize | More ▾
☐	▸	T[redacted]	Message Recipient		📱 ✉	Authorize | More ▾
☐	▸	t[redacted]	Sub-user	1[redacted]	📱 ✉	Authorize | More ▾
☐	▸	t[redacted]	Sub-user	1[redacted]	📱 ✉	Authorize | More ▾
☐	▸	t[redacted]	Collaborator	1[redacted]	📱 ✉	Authorize | More ▾

View collaborator information in the expanded drawer

Viewing collaborator information in the expanded drawer

You can expand to view sub-user information, which includes user groups, message subscriptions, login protection, operation protection, MFA device status, and console access status.

1. On the User List management page, locate the collaborator you wish to view.
2. Click on the "▶" icon in the details column on the left.
3. In the expanded drawer, you can view the sub-user's related information, thus completing the operation of viewing collaborator information in the drawer.

Viewing Collaborator Information through User Details

On the user details page, you can view detailed information about the sub-user, including basic information, quick operations and quick login entries, permissions, and services.

1. On the User List management page, locate the collaborator you wish to view.
2. Click on the username to enter the user details page.

3. On the User Details page, view the detailed information of the collaborator.

Deleting Collaborators

Last updated：2023-08-31 18:39:44

Scenario

When you no longer require a collaborator, you can remove them. Upon removal, the collaborator will no longer possess management permissions for resources under the root account.

Preparations

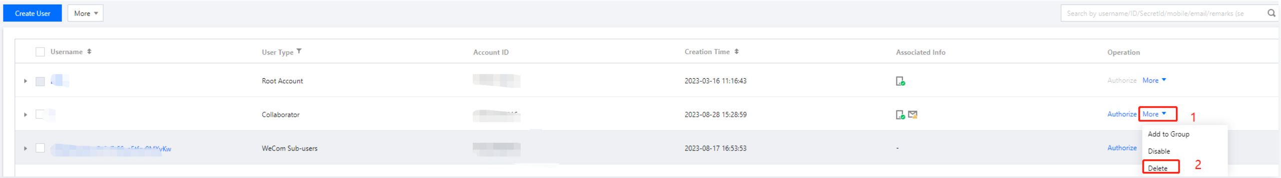
If the collaborator has API keys, you need to disable and delete the API keys first. For more information, see the Deleting Sub-account API Keys section.

Instructions

Deleting a single collaborator

Deletion via User List Page

1. Log in to the Cloud Access Management Console as the root account or a sub-account with **QcloudCamFullAccess policy** permissions.
2. On the **User List** page, locate the collaborator you wish to remove and click on **More** > **Delete** in the operation column.

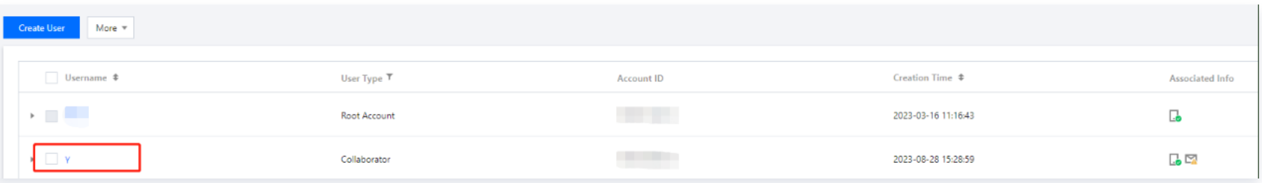


Username	User Type	Account ID	Creation Time	Associated Info	Operation
[redacted]	Root Account	[redacted]	2023-03-16 11:16:43		Authorize More
[redacted]	Collaborator	[redacted]	2023-08-28 15:28:59		Authorize More
[redacted]	WeCom Sub-users	[redacted]	2023-08-17 16:53:53	-	Authorize

3. In the user deletion window, simply click **Delete**.

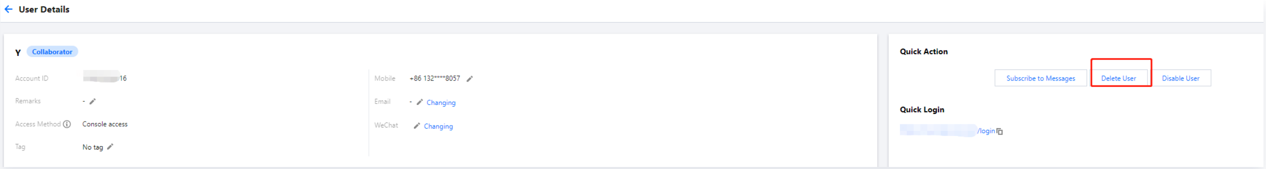
Deletion via User Details Page

1. Log in to the Cloud Access Management Console as the root account or a sub-account with **QcloudCamFullAccess policy** permissions.
2. Locate the collaborator you wish to remove, click on their username to navigate to their user details page.



Username	User Type	Account ID	Creation Time	Associated Info
[redacted]	Root Account	[redacted]	2023-03-16 11:16:43	
Y	Collaborator	[redacted]	2023-08-28 15:28:59	

3. In the Quick Action module of the User Details page, click **Delete User**.



Y Collaborator

Account ID [redacted]16

Remarks -

Access Method Console access

Tag No tag

Mobile +86 132****8057

Email - Changing

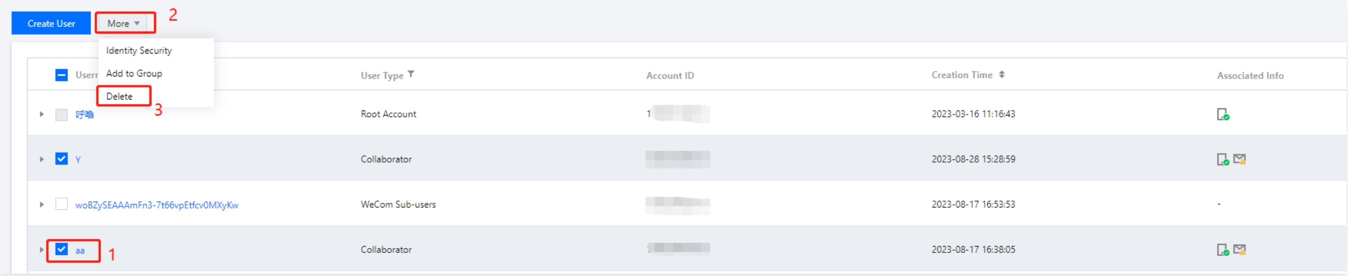
WeChat Changing

[redacted]/login

4. In the user deletion window, simply click **Delete**.

Deleting multiple collaborators

1. Log in to the Cloud Access Management Console as the root account or a sub-account with **QcloudCamFullAccess policy** permissions.
2. On the **User List** page, select the collaborator you wish to remove, then click on **More** > **Delete** at the top of the user list.



	Userr	User Type	Account ID	Creation Time	Associated Info
☐	呼啸	Root Account	[redacted]	2023-03-16 11:16:43	
☑	Y	Collaborator	[redacted]	2023-08-28 15:28:59	
☐	woBZySEAAAmFn3-7t66vpEtfcv0MXyKw	WeCom Sub-users	[redacted]	2023-08-17 16:53:53	-
☑	aa	Collaborator	[redacted]	2023-08-17 16:38:05	

3. In the user deletion window, simply click **Delete**.

Switching Collaborator Identities

Last updated：2023-08-31 18:40:12

Scenario

This document describes how to switch the identity of the root account to which a collaborator belongs to manage the resources under the corresponding root account within the scope of permissions.

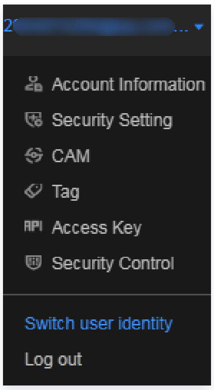
Preparations

The logged-in account is a collaborator of another root account.

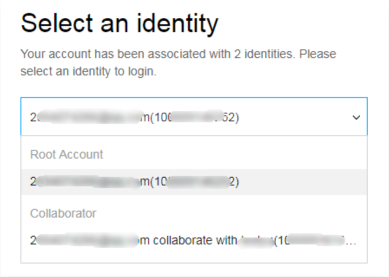
> **Note**
> For creating a collaborator, please refer to Creating a Collaborator.

Instructions

1. Navigate to the Tencent Cloud Management Console page and move the cursor to the account icon in the upper right corner of the page.
2. In the pop-up dropdown menu, click **Switch User identity**, as shown in the figure below:



3. On the select an identity page, click ∨ on the right of the account information. Select the root account identity that needs to be managed as shown below:


Select an identity

Your account has been associated with 2 identities. Please select an identity to login.

2[redacted]m(10[redacted]52)

Root Account

2[redacted]m(10[redacted]2)

Collaborator

2[redacted]m collaborate with [redacted](10[redacted]...

4. Click **Login** to complete the collaborator identity switch operation.

Message Recipients

Creating Message Recipient

Last updated：2023-08-31 18:40:36

Scenario

This document describes how to create a message recipient. A message recipient is a type of sub-accounts that cannot log in to the Tencent Cloud console or access the console programmatically. It can only receive messages through the contact method configured by the root account.

Instructions

1. Log in to the Cloud Access Management Console and select **Users** > User List from the left sidebar to navigate to the user list management page.
2. On the User List page, click **Create User** to navigate to the Create User page.
3. On the Create User page, click **Custom Create** to navigate to the Select Type page.
4. On the Select Type page, click **For Message Reception Only** to navigate to the Enter User Information page.
5. On the User Information page, enter the username, remarks, mobile number, and email. The remarks field is optional.
6. Click **Complete** to finish creating the message recipient.

Message Recipient Message Subscriptions

Last updated：2023-08-31 18:41:07

Scenario

This document describes how to verify message channels and set message subscription for recipients. Message recipients must first verify the message channel before they can receive messages. Message recipients will receive messages after they are subscribed and have verified the message channel.

Preparations

You have logged into the Cloud Access Management Console and navigated to the User List management page.

Instructions

Verifying message channel

1. On the User List management page, locate the recipient who needs to subscribe to the messages.
2. Click on the user's nickname to enter the user details page.
3. On the user details page, click **Replace - Resend Verification Link** under the user information bar.
    - Mobile: The system will send a verification message to the recipient's set mobile number. The user can complete the mobile message channel verification by confirming the link received in the verification message.
    - Email: The system will send a verification message to the recipient's set email address. The recipient can complete the email channel verification by confirming the link in the verification message.
    - Allow WeChat to receive notifications: After completing email verification, the system will send an email containing a QR code to the recipient's set email. Scanning the QR code with WeChat and following the WeChat Official Account will complete the verification of the WeChat message channel.

Setting message subscriptions

1. On the User List management page, locate the recipient who needs to subscribe to the messages.
2. Click on the **User Nickname** to access the user details page.
3. On the user details page, click **Subscribe to Messages** in the quick operations bar on the right.
4. A **Subscribe to Messages** window will pop up. You can select the message types here. Click ▼ to expand for granular selection options.
5. Click **OK** to finalize the subscription message configuration.

Setting Message Recipient User Groups

Last updated：2023-08-31 18:42:04

Scenario

This document describes how to add or remove message recipients from user groups to have them receive or stop receiving message notifications.

Preparations

You have logged into the Cloud Access Management Console and navigated to the User List management page.

Instructions

Adding message recipients to user groups

You can add a message recipient to the user group and the message recipient will receive all notifications set for the group.

1. On the User List management page, locate the message recipient you wish to add to the group.
2. Click on **More Operations** in the operation column, then select **Add to Group**.
3. In the pop-up window for adding to a group, select the user groups you wish to add.
4. Click **OK** to finalize the addition to the group.

Removing message recipients from user groups

You can stop a message recipient from receiving message notifications set for a user group by removing the message recipient from the user group.

1. On the User List management page, locate the message recipient you wish to remove from the group.
2. Click on the name of the message recipient to enter the user details page.
3. On the user details page, click **User Group** and locate the group you wish to remove.
4. Click **Remove from Group** in the operation column on the right, then click **Confirm Removal** to complete the removal of the message recipient from the user group.

Deleting Message Recipients

Last updated：2023-08-31 17:07:28

Scenario

This document describes how to delete one or multiple message recipients. After deletion, the user(s) will no longer receive messages from the root account.

Preparations

You have logged into the Cloud Access Management Console and navigated to the User List management page.

Instructions

Delete a message recipient

1. On the User List management page, locate the message recipient(s) you wish to delete.
2. Click **More Actions** > **Delete** in the operation column on the right to delete a single message recipient.

Delete multiple message recipients

1. On the User List management page, select the message recipients you wish to delete from the left side.
2. Click **More Actions** > **Delete** at the top left.
3. Click **Confirm Deletion** to complete the removal of the message recipient(s).

User information

Last updated：2023-08-31 17:08:25

Scenario

This document describes how to view and modify sub-account information including the user name, notes, and mobile phone number.

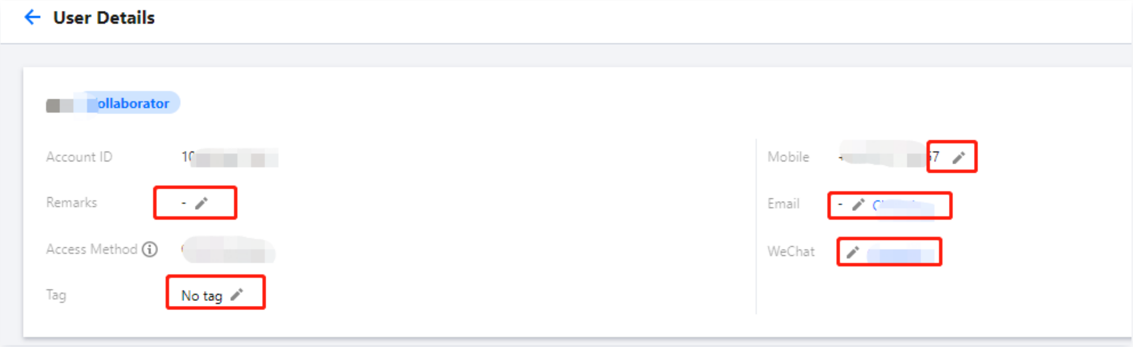
Instructions

Viewing User Information

1. Log in to the Cloud Access Management Console and navigate to the User List management page. Locate the sub-account whose information you wish to view.
2. Click on the **username** to access the user's detailed information page.
3. At the top of the page, you can view the current sub-account's user information, including the username, notes, mobile phone number, email, and whether WeChat notifications are allowed.

Modifying User Information

1. Log in to the Cloud Access Management Console and navigate to the User List management page. Locate the sub-account whose information you wish to modify.
2. Click on the **username** to enter the user details page. Click the corresponding modification entry to update the user information:



Modifying Information	Modification Entry	Note
Username	Edit Information in the Upper Right	Modify the username of the current collaborator. The sub-user's username cannot be changed as it is used for logging in.
Remarks		Modify the remark information of the current sub-account.
Mobile	Following the information ✎	To modify the mobile phone information bound to the current sub-account, this phone can be used to receive primary account notifications and identity verification before sensitive operations.
Email		Modify the current sub-account's bound email information. This email can be used to receive primary account notifications.
WeChat		Modify the current sub-account's WeChat notification status.

3. Click **Confirm** to complete the user information modification. You can find your sub-account on the User List management page by searching for the updated username, mobile number, notes, or email.

Associated Documents

If you wish to learn how to subscribe to messages for a sub-account, please refer to Sub-user Message Subscription, Collaborator Message Subscription, and Message Recipient Subscription.

User Settings

Password Rules

Last updated：2023-08-31 17:09:55

Background Information

Tencent Cloud does not store your plaintext password. Instead, it retains the value after salting and hashing with SHA256, ensuring that your password will not be exposed to anyone.

Scenario

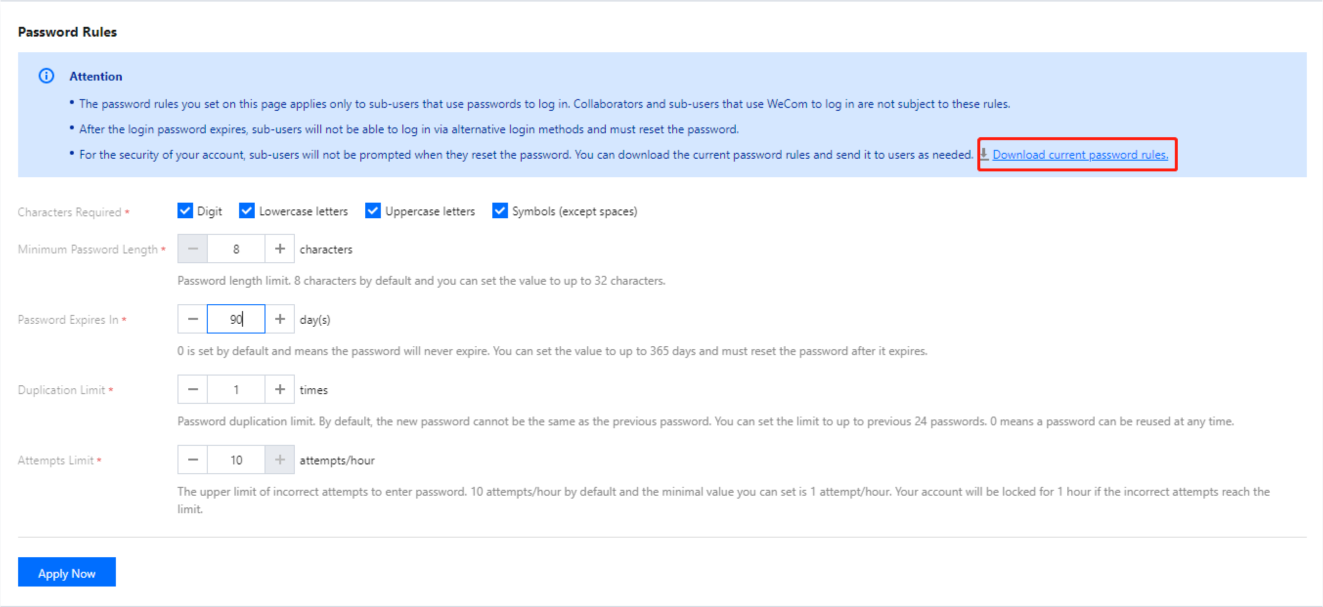
This task guides you through modifying the password rules for sub-users via the Cloud Access Management Console, including the complexity, length, and validity period of the password. If the password rules are not modified, the default settings will be applied.
In the following password setting scenarios, you need to follow the password rules that have been set:

- When defining the creation of a sub-user, the **Tencent Cloud Console Access** and **Custom Password** options are selected.
- When resetting the login password for a sub-user, the **Customize Password** option is selected.

Instructions

1. Log in to the Cloud Access Management Console, and in the left sidebar, select **Users** > User Settings to enter the User Settings page.
2. In the **Password Rules** module, modify specific rules such as the complexity, length, and validity period of the password.
3. Click **Apply Now**, and the password rules will take effect. You will need to follow these password rules the next time you reset your password.

> **Note**
> - The password policy you establish in this module only applies to sub-users who log in using passwords. This rule does not apply to collaborators or sub-users who log in by scanning the WeCom QR code.
> - After the login password expires, sub-users will not be able to log in via other login methods and must reset the password.
> - To ensure the security of your account, the detailed password rules will not be displayed when a sub-user resets their password. The root account, administrator, or a sub-account with the cam:GetPasswordRules interface permission can download the current password rules from the password rules page and distribute them to the necessary users, as shown below:



Password Rules

Attention

- The password rules you set on this page applies only to sub-users that use passwords to log in. Collaborators and sub-users that use WeCom to log in are not subject to these rules.
- After the login password expires, sub-users will not be able to log in via alternative login methods and must reset the password.
- For the security of your account, sub-users will not be prompted when they reset the password. You can download the current password rules and send it to users as needed. Download current password rules.

Characters Required * ☑ Digit ☑ Lowercase letters ☑ Uppercase letters ☑ Symbols (except spaces)

Minimum Password Length * 8 characters

Password length limit. 8 characters by default and you can set the value to up to 32 characters.

Password Expires In * 90 day(s)

0 is set by default and means the password will never expire. You can set the value to up to 365 days and must reset the password after it expires.

Duplication Limit * 1 times

Password duplication limit. By default, the new password cannot be the same as the previous password. You can set the limit to up to previous 24 passwords. 0 means a password can be reused at any time.

Attempts Limit * 10 attempts/hour

The upper limit of incorrect attempts to enter password. 10 attempts/hour by default and the minimal value you can set is 1 attempt/hour. Your account will be locked for 1 hour if the incorrect attempts reach the limit.

WeChat Restrictions

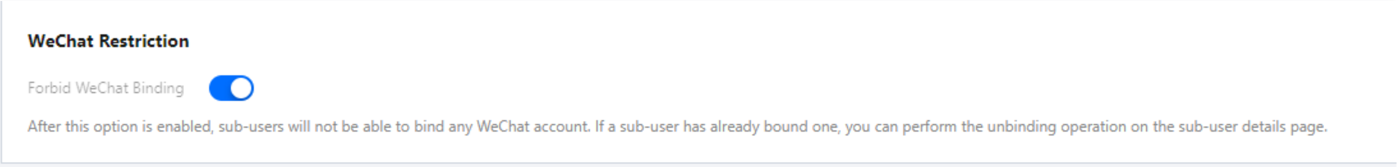
Last updated：2023-08-31 17:14:03

Scenario

This document provides instructions on how to restrict sub-users from binding with WeChat. Once the WeChat restriction is enabled, sub-users will not be permitted to bind with WeChat. If a sub-user has already bound with WeChat, you can unbind it from their user details page.

Instructions

1. Log in to the Cloud Access Management Console, navigate to **Users** > User Settings page, and locate the **WeChat Restriction** setting.
2. If you do not want to allow sub-users to bind with WeChat, you can enable the **Prohibit WeChat Binding** option. Once enabled, sub-users who have not yet bound with WeChat will receive a notification that they cannot bind when they attempt to do so.
3. Sub-users who have already bound with WeChat will not be restricted from using it. However, you can unbind WeChat from their user details page. There are two prerequisites for unbinding WeChat, as follows:
   - If a sub-user is only bound with WeChat and not with a mobile number, they will be unable to verify their identity for sensitive operations after unbinding from WeChat. Therefore, it is necessary to supplement their account with a mobile number.
   - If the current user account protection (login protection or operation protection) verification method is WeChat QR code verification, you need to go to the User List, access the user's details page, and navigate to **Security** > **Identity Security** to change to another verification method.
4. If you decide to allow sub-users to bind with WeChat again, simply disable the **Forbid WeChat Binding** option.



WeChat Restriction

Forbid WeChat Binding

After this option is enabled, sub-users will not be able to bind any WeChat account. If a sub-user has already bound one, you can perform the unbinding operation on the sub-user details page.

WeCom Restrictions

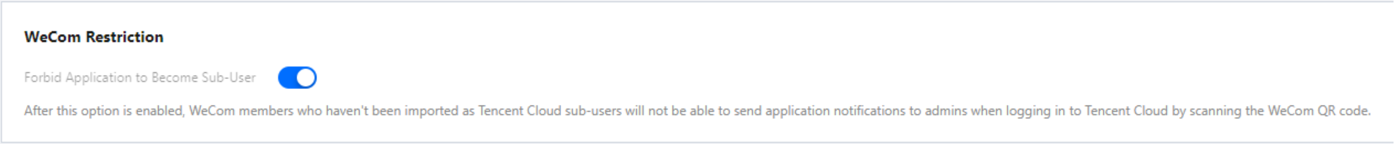
Last updated：2023-08-31 17:14:40

Scenario

If your Tencent Cloud account is linked to WeCom, but you do not wish for WeCom members to apply to become sub-users, you can set WeCom restrictions through this document to prevent WeCom members from applying to become sub-users with a single click.

Instructions

1. Log in to the Cloud Access Management Console, navigate to **Users** > User Settings page, and locate the **WeCom Restrictions** setting.
2. If you do not want WeCom members to apply to become sub-users, you can enable "Disallow Application to Become Sub-Users". WeCom members who have not been imported as Tencent Cloud sub-users will not be able to send application notifications to the administrator when logging into Tencent Cloud by scanning the WeCom QR code.
3. Sub-users who are already WeCom members are not restricted from logging in by scanning the WeCom QR code. However, you can still remove these WeCom sub-users from the user list.
4. If you want to allow WeCom members to become sub-users again, simply disable the **Forbid Application to Become Sub-User** setting.



WeCom Restriction

Forbid Application to Become Sub-User ●

After this option is enabled, WeCom members who haven't been imported as Tencent Cloud sub-users will not be able to send application notifications to admins when logging in to Tencent Cloud by scanning the WeCom QR code.

Login Status Management

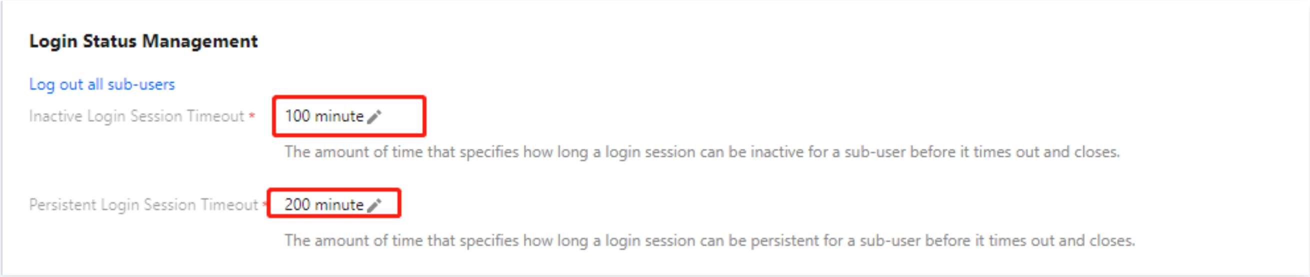
Last updated：2023-08-31 17:15:23

Scenario

This guide will walk you through the process of setting the session expiration time for a single login and operation of a sub-account via the Cloud Access Management Console. Once the session time has elapsed, you will need to log back into the console.

Instructions

1. Log in to the Cloud Access Management Console, navigate to **Users** > User Settings page, and locate the **Login Status Management** setting.
2. Click on the ✎ next to Login Persistence Time to set the duration for maintaining the login status.



Login Status Management

Log out all sub-users

Inactive Login Session Timeout * 100 minute ✎

The amount of time that specifies how long a login session can be inactive for a sub-user before it times out and closes.

Persistent Login Session Timeout * 200 minute ✎

The amount of time that specifies how long a login session can be persistent for a sub-user before it times out and closes.

setting type	Value Range	Note
Inactive Login Session Timeout	15 minutes to 12 hours	After a sub-user logs in, the session can be maintained for a certain duration without any activity. Once this duration is exceeded, the system will automatically log out.
Persistent Login Session Timeout	1 to 48 hours	The maximum session duration for a sub-user after login is set. If this duration is exceeded, the system will log out.

3. Click **Save** to complete the configuration.

Identity Security Management

Last updated：2023-08-31 17:16:25

Scenario

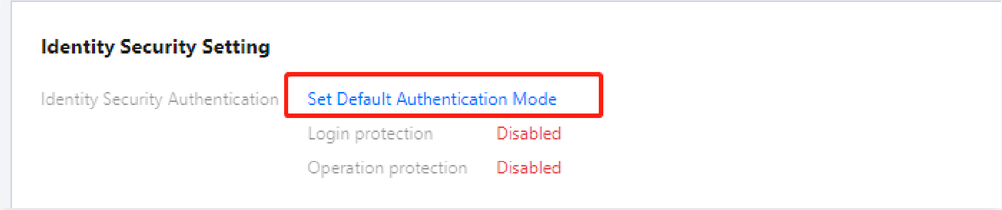
This guide will walk you through the process of setting up login protection and operation protection identity security authentication via the Cloud Access Management Console.

Enabling MFA on the user settings page is only applicable to newly created sub-users. For existing sub-users, you need to go to the **User Details** page, click on the **Security** tab, and manually enable MFA on the **Security** page to enhance account security.

Instructions

Enabling MFA for Newly Created Sub-Users

1. Log in to the Cloud Access Management Console, navigate to **Users** > User Settings page, and locate the **Identity Security Setting** option.
2. Click on **Set Default Authentication Mode** to enter the Identity Security Settings window.



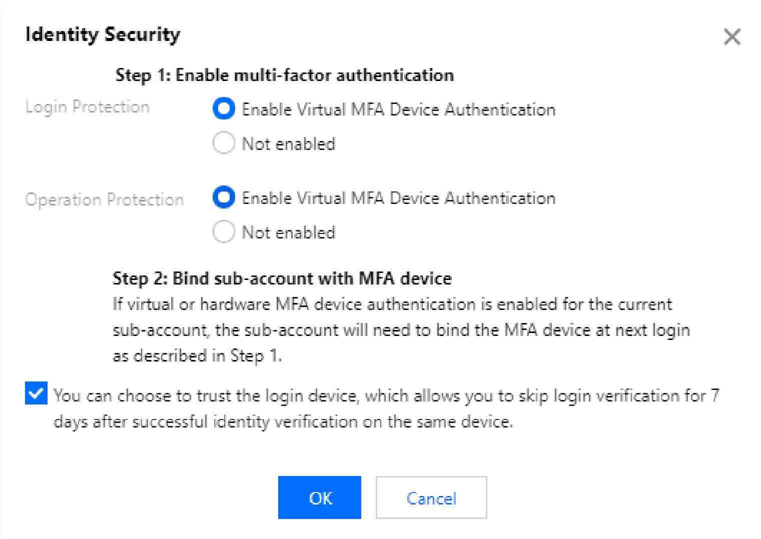
Identity Security Setting

Identity Security Authentication Set Default Authentication Mode

Login protection Disabled

Operation protection Disabled

3. Check the box to "Enable Virtual MFA Device Authentication" for the current sub-account, if necessary.



Identity Security

Step 1: Enable multi-factor authentication

Login Protection
● Enable Virtual MFA Device Authentication
○ Not enabled

Operation Protection
● Enable Virtual MFA Device Authentication
○ Not enabled

Step 2: Bind sub-account with MFA device

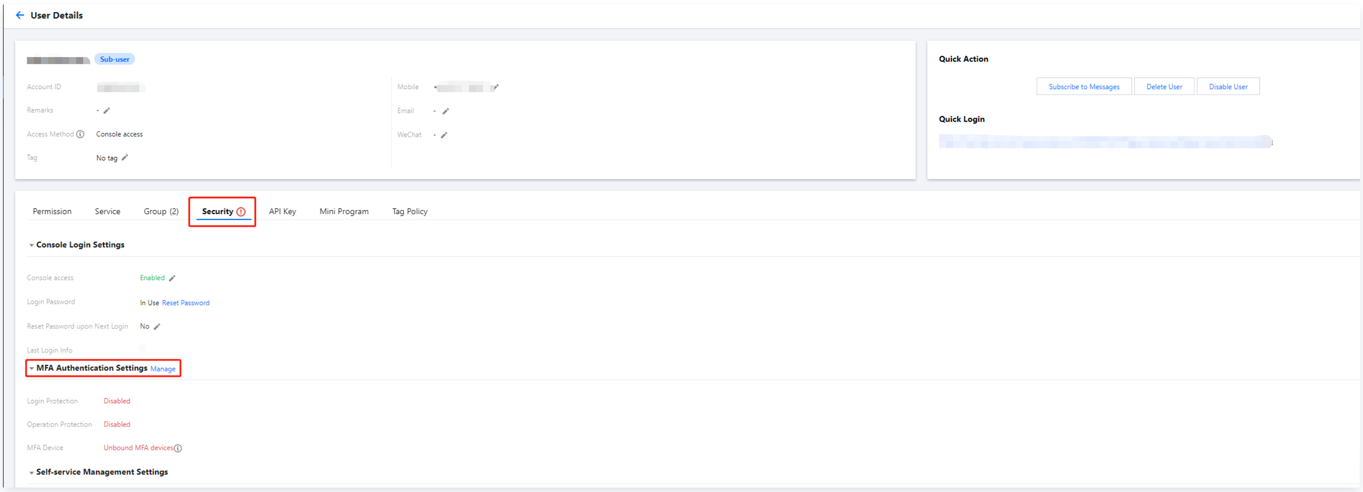
If virtual or hardware MFA device authentication is enabled for the current sub-account, the sub-account will need to bind the MFA device at next login as described in Step 1.

☑ You can choose to trust the login device, which allows you to skip login verification for 7 days after successful identity verification on the same device.

4. Click **OK** to complete the configuration. The sub-account will bind the MFA device according to the settings at the next login.

Enabling MFA for Existing Sub-Users

1. Log in to the Cloud Access Management Console, navigate to **Users** > User List page, find the sub-user and click on the user name to enter the **User Details** page, select **Security** to set up MFA authentication.



User Details

[redacted] Sub-user

Account ID [redacted]

Remarks -

Access Method Console access

Tag No tag

Mobile [redacted]

Email -

WeChat -

Quick Action

Quick Login

[redacted]

Console Login Settings

Console access Enabled

Login Password In Use Reset Password

Reset Password upon Next Login No

Last Login Info

MFA Authentication Settings Manage

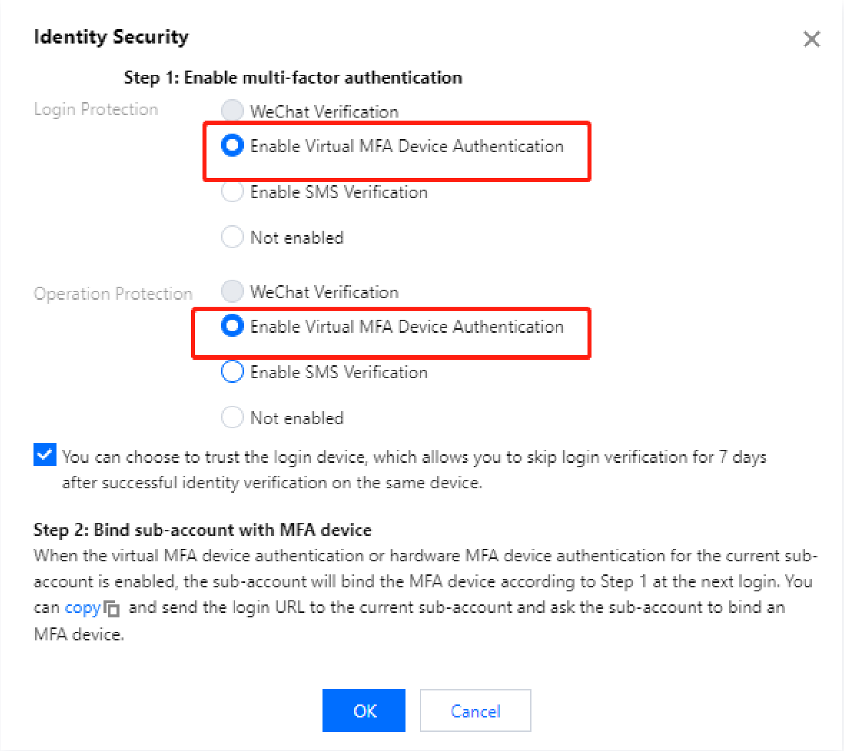
Login Protection Disabled

Operation Protection Disabled

MFA Device Unbound MFA devices

Self-service Management Settings

2. Click on **Manage** to open the **Identity Security** window, and select whether to "Enable Virtual MFA Device Authentication" for the current sub-account based on your needs.



Identity Security

Step 1: Enable multi-factor authentication

Login Protection
○ WeChat Verification
● Enable Virtual MFA Device Authentication
○ Enable SMS Verification
○ Not enabled

Operation Protection
○ WeChat Verification
● Enable Virtual MFA Device Authentication
○ Enable SMS Verification
○ Not enabled

☑ You can choose to trust the login device, which allows you to skip login verification for 7 days after successful identity verification on the same device.

Step 2: Bind sub-account with MFA device

When the virtual MFA device authentication or hardware MFA device authentication for the current sub-account is enabled, the sub-account will bind the MFA device according to Step 1 at the next login. You can copy and send the login URL to the current sub-account and ask the sub-account to bind an MFA device.

3. Click **OK** to complete the configuration. Existing sub-users will bind the MFA device according to the settings at their next login.

Access Key

Root Account Access Key Management

Last updated：2024-02-01 21:37:31

Scenario

Access keys, also known as API keys, are security credentials required for user identity verification when accessing Tencent Cloud APIs. They are composed of a SecretId and SecretKey. If a user does not yet have an API key, it is necessary to create one in API Key Management, otherwise, the cloud API interface cannot be invoked.
This document provides guidance on how to create, disable/enable, delete API keys, and view the API key information of the main account.

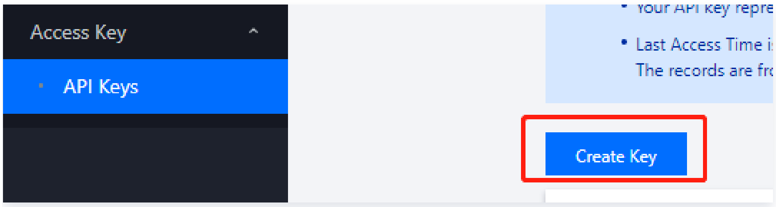
Preparations

You have logged in to the Cloud Access Management Console as the root account and navigated to the API Key Management page.

Instructions

Creating an API key for a root account

You can create an API key for the root account. Once created, the root account can manage resources under the account through the API, SDK, or other development tools.
On the API Keys page, click **Create Key** to complete the API key creation process. As shown below:



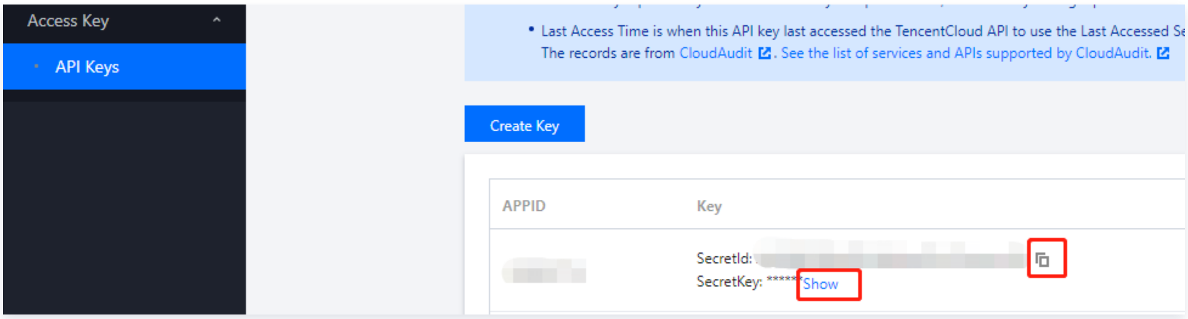
Note

- One root account can have at most two API keys.
- The root account API key represents your account identity and granted permissions, which is equivalent to your login password. Do not disclose it to others.
- An API key is an important credential for creating Tencent Cloud API requests. To keep your assets and services secure, store your keys appropriately, change them regularly, and delete old keys after creating new ones.

Viewing an API key of a root account

You can view and copy the `SecretId` and `SecretKey` of the API key of the root account. You can use the `SecretId` and `SecretKey` to use APIs, SDKs, or other developer tools to manage resources under the account.

1. On the API Keys page, click ⧉ to directly obtain and copy the SecretId.
2. In the key operation column, click **Show**, complete the identity verification, and you can obtain and copy the SecretKey. As shown in the figure below:



Access Key

API Keys

- Last Access Time is when this API key last accessed the TencentCloud API to use the Last Accessed Se
The records are from CloudAudit. See the list of services and APIs supported by CloudAudit.

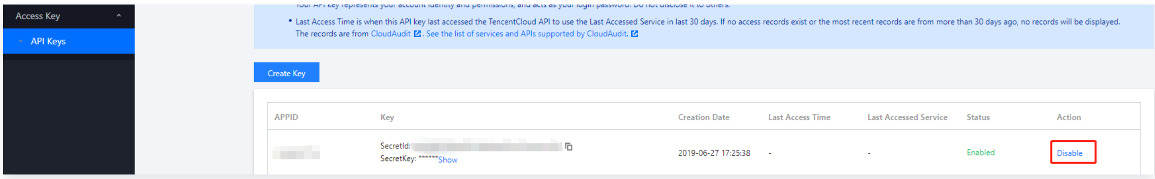
Create Key

APPID	Key
[redacted]	SecretId: [redacted] SecretKey: ***** Show

Disabling/Enabling root account API key

You can disable an API key of the root account. Tencent Cloud will block all requests that use the API key after it is disabled.

1. On the API Keys page, click **Disable** under the operation column. As shown below:



Access Key

API Keys

- Last Access Time is when this API key last accessed the TencentCloud API to use the Last Accessed Service in last 30 days. If no access records exist or the most recent records are from more than 30 days ago, no records will be displayed.
The records are from CloudAudit. See the list of services and APIs supported by CloudAudit.

Create Key

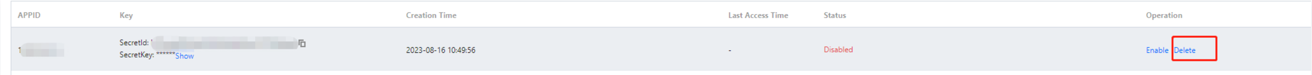
APPID	Key	Creation Date	Last Access Time	Last Accessed Service	Status	Action
[redacted]	SecretId: [redacted] SecretKey: ******Show	2019-06-27 17:25:38	-	-	Enabled	Disable

2. In the pop-up window, click **Disable** to complete the operation of disabling the access key.

> **Note**
> Click **Enable** under the operation column to activate the current key. Once enabled, you can manage resources under the account via API, SDK, or other development tools.

Deleting root account API key

1. On the API Keys page, click **Disable** in the operation column. If the API key you wish to delete is already disabled, you can proceed directly to Step 3.
2. In the pop-up window, click **Disable**.
3. On the API Key Management page, click **Delete** in the operation column. As shown below:



APPID	Key	Creation Time	Last Access Time	Status	Operation
1 [redacted]	SecretId: [redacted] SecretKey: ******Show	2023-08-16 10:49:56	-	Disabled	Enable Delete

4. In the pop-up window, click **Delete** to complete the deletion of the API key.

> **Note**
> Please note that an API key cannot be recovered once deleted.

Access Key

Last updated：2023-08-31 17:23:58

Scenario

This document describes how to create, enable/disable, delete, and view API keys for sub-users and collaborators.

Preparations

You have logged into the Cloud Access Management Console, navigated to the User List Console page, located the sub-user/collaborator that needs to be set up, clicked on the **User Name**, and entered the user details page.

Instructions

Creating API Key for Sub-account

You can create an API key for a sub-user/collaborator. After the API key is created, the sub-user/collaborator can use APIs, SDKs, or other developer tools to manage the resources under the root account within the scope of the configured permissions.

1. On the user details page, click **API Keys** to navigate to the API key management page.
2. On the API Key Management page, click **Create API Key** to complete the API key creation process.

> **Note**
> - Each sub-user/collaborator can have at most two API keys.
> - An API key is an important credential for creating Tencent Cloud API requests. To keep your assets and services secure, store your keys appropriately, change them regularly, and delete old keys after creating new ones.

Viewing Sub-account API Key

You can view and copy the SecretId and SecretKey information of the sub-user/collaborator's API key. The sub-user/collaborator can manage resources under the main account within the scope of permissions using the SecretId and SecretKey via APIs, SDKs, or other development tools.

1. On the user details page, click **API Keys** to navigate to the API key management page.
2. On the API Key Management page, you can view and copy the SecretId and SecretKey information of the API key. The API key is a crucial credential for constructing Tencent Cloud API requests. For the safety of your assets and services, please store your keys properly and change them regularly. Once you have replaced your keys, promptly delete the old ones.
   - SecretId: It can be directly viewed in the key column. Click ⧉ to copy and save the relevant information.
   - SecretKey: Click **Show** in the key column. After completing the identity verification, you can directly view it. Click ⧉ to copy and save the relevant information.

Enable/Disable Sub-account API Key

You can disable the API keys of sub-users and collaborators. Do note that Tencent Cloud will block all requests that use the API key after it is disabled.

1. On the user details page, click **API Keys** to navigate to the API key management page.
2. On the API Key Management page, click **Disable** in the operation column.
3. In the confirmation window that appears, click **Confirm** to complete the operation of disabling the access key.

> **Note**
> Click **Enable** under the operation column to activate the current key. Once activated, the sub-account/collaborator can manage resources under the master account within the scope of permissions via API, SDK, or other development tools.

Deleting Sub-account API Key

1. On the user details page, click **API Keys** to navigate to the API key management page.
2. On the API Key Management page, click **Disable** in the operation column. If the API key you want to delete is already disabled,

you can proceed directly to step 4.

3. In the confirmation window that appears, click **Confirm**.
4. On the API Key Management page, click **Delete** in the operation column to complete the deletion of the API key.

> **Note**
> Please note that an API key cannot be recovered once deleted.

Associated Documents

If you want to learn how to query sub-account information through the SecretId of the access key, please refer to Finding Sub-users through the Search Box and Finding Collaborators through the Search Box.

User Groups

Creating User Group

Last updated：2023-08-31 17:25:02

Scenario

A user group is a collection of users (sub-accounts) with similar functions. The primary account and sub-accounts with administrative privileges can create different user groups based on business needs, and manage users and their permissions more effectively through batch authorization, setting subscription messages, and so forth.

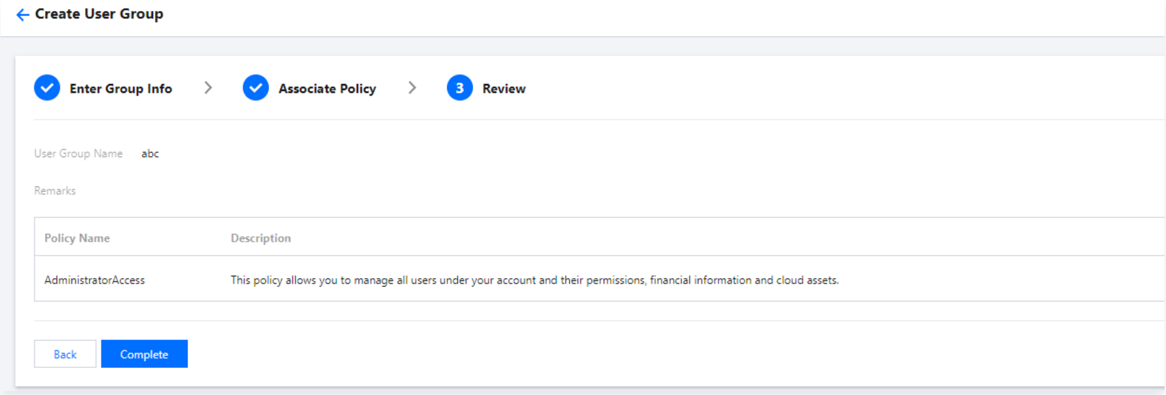
This document provides instructions on how to create a user group and associate it with a policy. You can assign your users to different user groups for group management. Users within a user group will manage resources under the primary account within the scope of their granted permissions.

Operations Guide

1. Log in to the Cloud Access Management Console and navigate to the User Group page.
2. Click on **Create User Group** to navigate to the page where you can fill in the user group information.
3. Enter the user group name and notes if any. The user group name is required.

> **Note**
> You can quickly find a specific user group in the user groups list by searching the user group name or the note you made for that user group.

4. Click **Next** to proceed to the Set User Group Permissions page.
5. Select the policy which you want to associate with this user group. You can select more than one.
6. Click **Next** to proceed to the review page.
7. Review the settings selected for the user group. Make any changes if needed.
8. After confirming that everything is correct, click **Complete** to finish creating the new user group.



User Group Name abc

Remarks

Policy Name	Description
AdministratorAccess	This policy allows you to manage all users under your account and their permissions, financial information and cloud assets.

Associated Documents

If you wish to understand how to manage sub-users and group authorizations through user groups, please refer to User Management and User Group Permission Settings.

If you wish to understand how to create sub-users, please refer to Custom Creation of Sub-Users.

Managing User Groups

Last updated：2023-08-31 17:25:53

Scenario

After creating and authorizing a user group, you can add/remove sub-accounts to/from it to quickly change user permissions.

- Upon adding a user to a user group, the user will inherit all permissions of that group.
- Upon removing a user from a user group, the user will no longer possess the permissions of that group.

Preparations

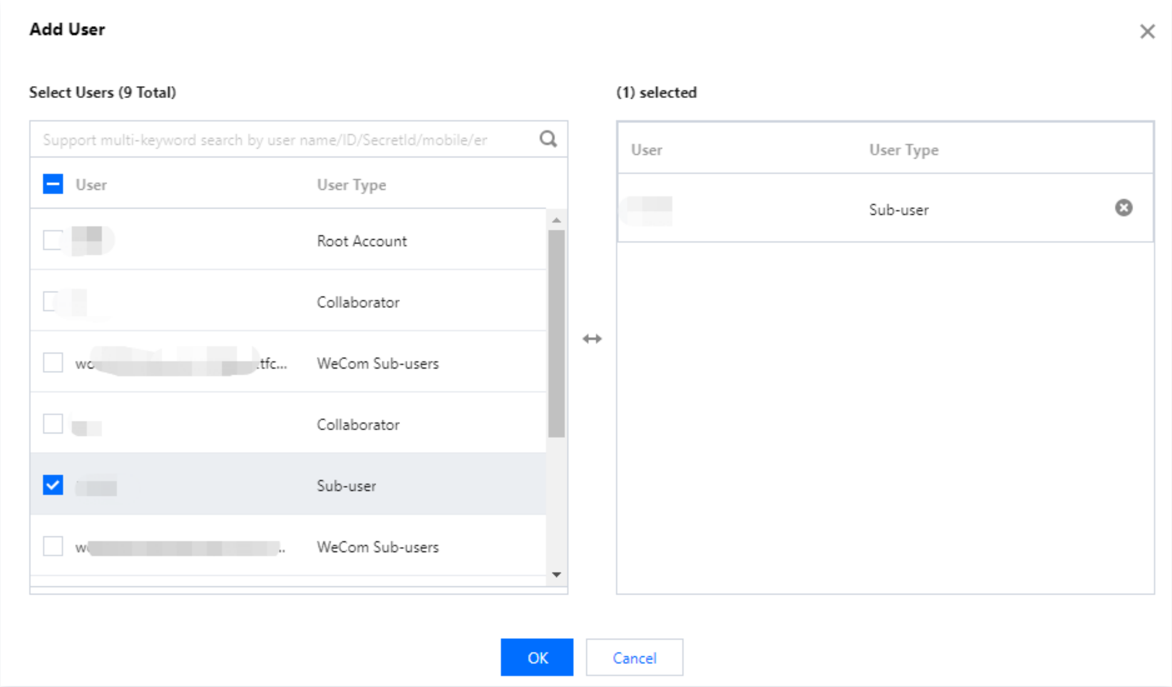
- You should already have a user group (if not, please Create a User Group).
- You should already have a sub-account. If not, please create a new sub-account.

Instructions

Adding user to user group

1. Log in to the Cloud Access Management Console and navigate to the User Group page.
2. Locate the target user group and click **Add User** in the operation column.
3. In the pop-up window, check the user to be added.
4. Click **OK** to finalize the addition of users to the user group.

> **Note**
> You may also click on the user group name and add users in the **Users** tab on the details page.



Add User

Select Users (9 Total)

Support multi-keyword search by user name/ID/SecretId/mobile/er

	User	User Type
☐	[redacted]	Root Account
☐	[redacted]	Collaborator
☐	wo[redacted]tfc...	WeCom Sub-users
☐	[redacted]	Collaborator
☑	[redacted]	Sub-user
☐	w[redacted]..	WeCom Sub-users

(1) selected

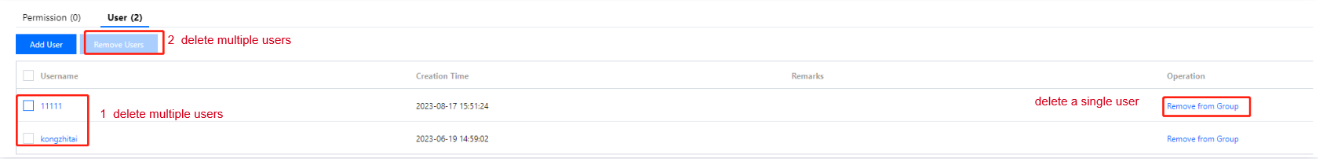
User	User Type
[redacted]	Sub-user

Removing user from user group

1. Log in to the Cloud Access Management Console and navigate to the User Group page.
2. Click the user group name to enter the user group details page.
3. On the User Group Details page, click **Users** to navigate to the User List page.
4. Locate the user to be removed and click **Remove from Group** in the operation column on the right.
5. Click **Remove User** to complete the operation of deleting a single user from the user group.

Note

You can also select users and click **Remove Users** above the user list to delete multiple users at once.



2 delete multiple users

Username	Creation Time	Remarks	Operation
□ 11111	2023-08-17 15:51:24		Remove from Group
□ kongzhitai	2023-06-19 14:59:02		Remove from Group

1 delete multiple users

delete a single user

Associating/Unassociating Policy with/from User Group

Last updated：2023-08-31 17:26:49

Scenario

After creating a user group and completing the authorization, you can add/remove policies for the user group to quickly effectuate changes in the group's permissions. Sub-accounts under the user group will manage resources under the root account within the scope of the permissions they have been granted.

- When a policy is added to a user group, all users within that group will possess the permissions corresponding to that policy.
- When a policy is disassociated from a user group, all users within that group will no longer possess the permissions corresponding to that policy.

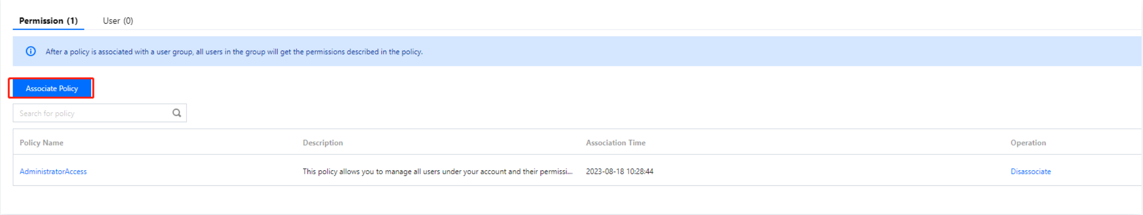
Preparations

You should already have a user group (if not, please Create a User Group).

Instructions

Associating policy with user group

1. Log in to the Cloud Access Management Console and navigate to the User Group page.
2. Find the target user group and click its name to enter the user group details page.
3. In the **Permissions** section of the User Group Details page, click **Associate Policy**.



Permission (1) User (0)

After a policy is associated with a user group, all users in the group will get the permissions described in the policy.

Associate Policy

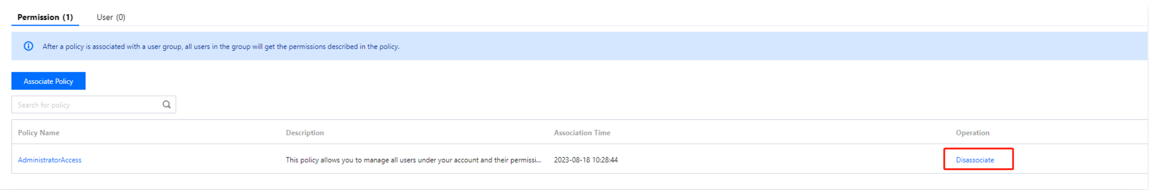
Search for policy

Policy Name	Description	Association Time	Operation
AdministratorAccess	This policy allows you to manage all users under your account and their permissi...	2023-08-18 10:28:44	Disassociate

4. In the Associate Policy dialog box, select the policies you want to add (multiple selections allowed), and click **OK** to complete the process of adding policies to the user group.

Unassociating policy from user group

1. Log in to the Cloud Access Management Console and navigate to the User Group page.
2. Find the target user group and click its name to enter the user group details page.
3. In the **Permissions** section of the User Group Details page, locate the policy you wish to disassociate and click **Disassociate** on the right.



Permission (1) User (0)

After a policy is associated with a user group, all users in the group will get the permissions described in the policy.

Associate Policy

Search for policy

Policy Name	Description	Association Time	Operation
AdministratorAccess	This policy allows you to manage all users under your account and their permissi...	2023-08-18 10:28:44	Disassociate

4. After confirming, click **OK** to complete the process of disassociating the policy from the user group.

Deleting User Groups

Last updated：2023-08-31 17:27:22

Scenario

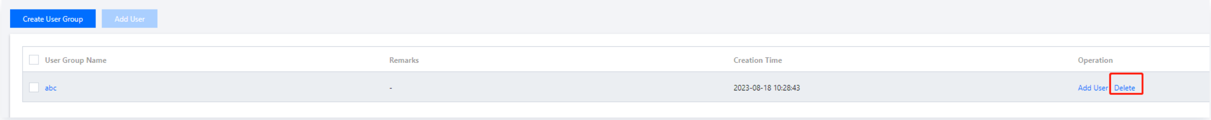
When a user group is no longer required, it can be removed. Deleting a user group does not eliminate the users within the group, but they will lose the permissions obtained through the group and will not receive any SMS or email notifications from the group.

Preparations

A user group already exists.

Instructions

1. Log in to the Cloud Access Management Console and navigate to the User Group page.
2. On the User Group Management console page, locate the user group that needs to be deleted.
3. Click **Delete** in the **Operation** column on the right to complete the user group deletion process.



Create User Group | Add User

□ User Group Name	Remarks	Creation Time	Operation
□ abc	-	2023-08-18 10:28:43	Add User Delete

Role

Role Overview

Last updated：2024-01-26 15:39:56

Role Overview

A role in CAM is a type of virtual user, distinct from entity users such as sub-accounts, collaborators, or message recipients. Similar to these users, a role can also be granted policies.

A role can be assumed by any Tencent Cloud account and is not exclusively associated with a specific account. Roles do not have associated long-term credentials (passwords or access keys). The primary account only needs to use long-term credentials when applying for a role. When a user assumes a role, a temporary credential is dynamically created and provided to the user for corresponding access. This allows the user to access their cloud resources by signing with a temporary key to call the open APIs of Tencent Cloud's basic services.

Use Cases

Entities that can apply to assume a role are referred to as role entities. Currently, Tencent Cloud role entities are divided into three categories: Tencent Cloud accounts, product services that support the role function, and identity providers. The corresponding scenarios are as follows:

- You want to grant temporary resource access permissions to users in your account, or grant users in another Tencent Cloud primary account access to resources in your account.
- You may need to grant Tencent Cloud product services access to your resources, but you may not want to embed long-term keys in the product services due to the security risks associated with key rotation difficulties and potential exposure from interception.
- If your enterprise or organization already has its own account system and wishes to manage the use of Tencent Cloud resources by its members, Tencent Cloud supports the use of Identity Providers (IdP) so you don't have to create a CAM sub-user for each member within your Tencent Cloud account.

Concepts

Last updated：2024-01-26 15:50:28

Before you start using roles, you need to understand some basic terms, including roles, service roles, custom roles, role entities, and permission policies. For more terminology, please see the Glossary.

Role

A role is a virtual identity with a set of permissions. It is used to grant access to services, operations, and resources in Tencent Cloud to role entities. These permissions are attached to the role, not to specific users or user groups.
CAM supports the following four types of roles:

Type	Custom role		Tencent Cloud Product Service	
	Tencent Cloud account	Identity Providers	Service role	Service-Linked Role
Description	A role defined by the user, where the user has the flexibility to determine the role entity and role permissions.		A role predefined by Tencent Cloud services. The service role requires user authorization, and the service can access user resources by assuming the service role.	
Entity	Create a Tencent Cloud account	Identity Providers	Tencent Cloud services	Tencent Cloud services
Authorization Policy Modification	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable
Supports deletion	This feature is supported.	This feature is supported.	This feature is supported.	Supported (deletion is not supported when the role has associated resources)

Service role

A service role is a unique type of CAM preset role directly provided by various Tencent Cloud services. The associated permissions of a service role are predefined by the relevant product service. Once you assign a service role to a product service, that service can fully represent you in calling other Tencent Cloud product services within the scope of the service role's permissions. Service roles make it easier for you to use services, as you don't have to manually add permissions during the role assignment process, you only need to decide whether to grant the service the relevant permissions of the service role.
In the process of assigning a service role to a related product service, the relevant permissions and role entities of the service role have been defined. Unless otherwise specified, only this service can assume the role. The predefined elements of a service role include the role name, role entity, and permission policy. To check whether a Tencent Cloud product service supports the use of service roles, please see CAM-Supported Products.

Service-Linked Role

A Service-Linked Role is a unique type of service role that is directly associated with a Tencent Cloud service. It is predefined by the service and has all the permissions the service needs to call other Tencent Cloud services on your behalf. The Service-Linked Role also defines how to create, modify, and delete the Service-Linked Role. The service can automatically create or delete roles. It may allow you to create, modify, or delete roles during the service's wizard or process. Alternatively, it may require you to create or delete roles using Tencent Cloud. Regardless of the method used, service-linked roles make it easier for you to set up services because you do not have to manually add the permissions the service required to perform operations.

Custom role

A custom role is a role defined by the user in CAM. The role name, role entity, and role permissions are all determined by the user. Custom roles allow you to allocate access and usage permissions for your cloud resources with greater freedom and flexibility.

Objects that are granted a role can only have the corresponding permissions when using the role, avoiding the security risks caused by persistent keys.

Role Entity

A role entity is an object that is allowed to carry the permissions of a role. You can edit the role entity of a role, add or delete corresponding objects to allow or deny them to play the role to access your Tencent Cloud resources. The role entity types currently supported by Tencent Cloud are: Tencent Cloud account and Tencent Cloud services that support roles. To check whether a Tencent Cloud product service supports the use of service roles, please see Products that support CAM .

Permission Policy

It is a permission document in JSON format. You can define the operations and resources that a role can use in the permission policy. The rules of this document depend on the CAM policy language rules.

Trust policy

It is a permission document in JSON format. In the trust policy, you can define the entities that can assume the role and the conditions that must be met when assuming the role. The rules of this document depend on the CAM policy language rules.

Note:
Please exercise caution when granting AssumeRole permissions to sub-accounts. If a sub-account has unrestricted AssumeRole permissions, it can impersonate all roles (including service roles and service-related roles), which can easily lead to excessive permissions.

Creating Role

Last updated：2024-01-26 15:55:42

Scenario

This document outlines how to create roles using either the Cloud Access Management Console or the CAM API. Once successfully created, these roles can manage resources under the primary account within their granted permissions.

Preparations

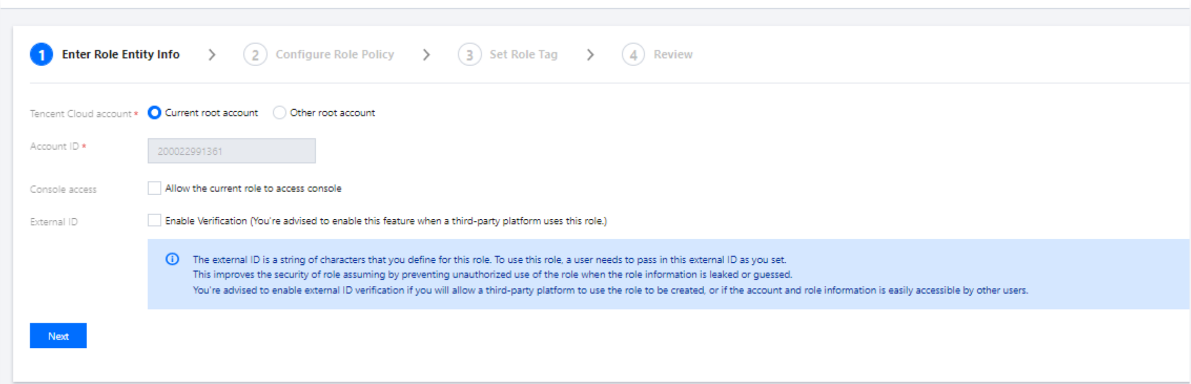
You have logged into the Cloud Access Management Console and navigated to the Roles list page.

Instructions

Creating a Role via Console

Creating a Role for Tencent Cloud root account

1. On the Roles list page, click **Create Role**.
2. In the pop-up **Enter Role Entity Info** window, select **Tencent Cloud Account** as the role carrier, and proceed to the role information entry page.



Tencent Cloud account * ● Current root account ○ Other root account

Account ID * 200022991361

Console access □ Allow the current role to access console

External ID □ Enable Verification (You're advised to enable this feature when a third-party platform uses this role.)

The external ID is a string of characters that you define for this role. To use this role, a user needs to pass in this external ID as you set.
This improves the security of role assuming by preventing unauthorized use of the role when the role information is leaked or guessed.
You're advised to enable external ID verification if you will allow a third-party platform to use the role to be created, or if the account and role information is easily accessible by other users.

3. On the "Enter Role Entity Info" page, fill in the following information and click **Next**.
   - Tencent Cloud account : Select either **Current root account** or **Other root account**.
   - Account ID: Enter the ID of the primary account you authorize to assume roles and access your Tencent Cloud resources. The default input is your primary account ID.
   - Console access: If selected, the current role will be granted access to the console.
   - External ID: If the role you are creating is to be assigned to a third-party external platform, or if the account and role information is easily accessible to other users, it is recommended that you enable external ID verification. Once enabled, you will need to enter an external ID.
4. Within the policy list, select the policies you wish to assign to the role you are creating, then click **Next**.
5. Mark the tag key and tag value of the role, then click **Next**.
6. Enter your role name, review the role carrier and policy information for accuracy, and click **Complete** to finish creating your custom role.

> **Note**
> If you intend to assign roles to other Tencent Cloud sub-accounts, please see Assign Role Play Policies to Sub-accounts.

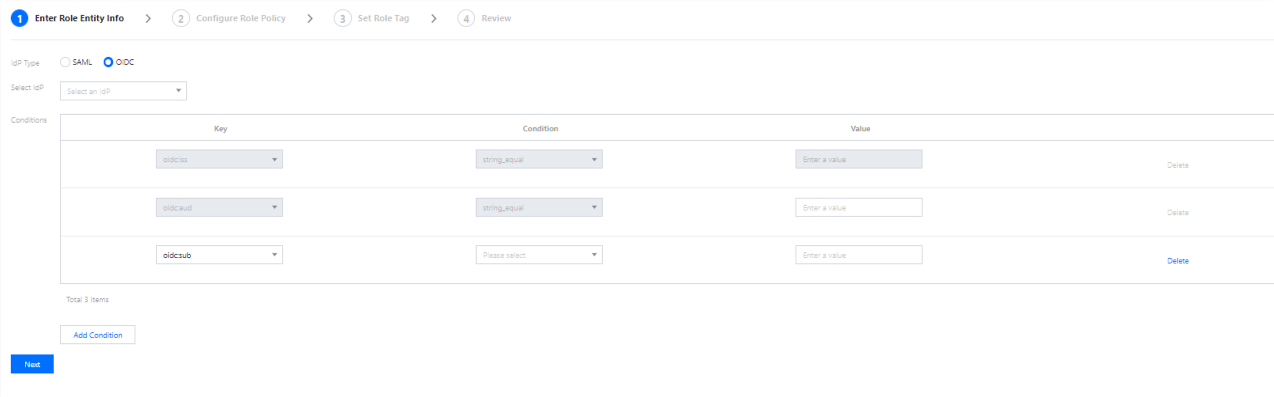
Creating a role for a Tencent Cloud Service

1. On the Roles list page, click **Create Role**.
2. In the pop-up window for selecting the role carrier, choose **Tencent Cloud services** as the role carrier and proceed to the role information entry page. To check whether Tencent Cloud services support the use of service roles, please see CAM-supported Products.

3. In the list of service products that support role functionality, select the services you need as role carriers and click **Next**.
4. Within the policy list, select the policies you wish to add to the current role to configure its policies, then click **Next**.
5. Mark the tag key and tag value of the role, then click **Next**.
6. Enter your role name, review the information related to the role you are about to create, and click **OK** to complete the creation of the custom role.

Creating a role for an identity provider

1. On the Roles list page, click **Create Role**.
2. In the pop-up window for selecting the role carrier, choose **Identity Provider** as the role carrier and proceed to the role information entry page.
   Identity Provider refers to the identity provider you have successfully created. Select which identity provider the role is being created for this time.



1 Enter Role Entity Info > 2 Configure Role Policy > 3 Set Role Tag > 4 Review

IdP Type ○ SAML ● OIDC

Select IdP: Select an IdP

Conditions

Key	Condition	Value	
oidc:iss	string_equal	Enter a value	Delete
oidc:aud	string_equal	Enter a value	Delete
oidc:sub	Please select	Enter a value	Delete

Total 3 items

3. Select the identity provider type and the specific identity provider, configure usage conditions as needed, and click **Next**.
   - Identity Provider Type: Supports both SAML and OIDC.
   - Select Identity Provider: Choose the identity provider for which you are creating a role.
   - Console Access (Optional): Manage whether the role is allowed to log in to the Tencent Cloud Management Console. By default, all roles can access Tencent Cloud programmatically.
   - Conditions (Optional): The circumstances under which the identity provider can use this role. For more information, see Using Conditions .
4. Within the policy list, select the policies you wish to add to the current role to complete the permission configuration, then click **Next**.
5. Mark the tag key and tag value of the role, then click **Next**.
6. Enter your custom role name, review the information related to the role you are about to create, and click **OK** to complete the creation of the custom role.

Creating a role using API

Creating a role for Tencent Cloud account

You can create a role by using CAM APIs in Tencent Cloud. Here we explain the process with a typical use case.
For example, Company A wants to outsource its Ops Engineer position to Company B. The person taking the position needs the access to all Company A's CVM resources located in the Guangzhou region.
Company A's enterprise account CompanyExampleA (ownerUin:12345) creates a role and sets the role entity to Company B's enterprise account CompanyExampleB (ownerUin: 67890).

1. `CompanyExampleA` (ownerUin: 12345) calls the `CreateRole` API to create a role with `DevOpsRole` as the `roleName` . The parameter `policyDocument` (role trust policy) is configured as follows:

```
  {
"version": "2.0",
"statement": [
  {
   "action": "name/sts:AssumeRole",
    "effect": "allow",
      "principal": {
        "qcs": ["qcs::cam::uin/67890:root"]
   }
   }
    ]
   }
```

2. CompanyExampleA (ownerUin: 12345) needs to add permissions to the new role.
3. CompanyExampleA (ownerUin: 12345) creates a new policy `DevOpsPolicy` . The policy syntax is as follows:

```
     {
   "version": "2.0",
   "statement": [
     {
      "effect": "allow",
     "action": "cvm:*",
     "resource": "qcs::cvm:ap-guangzhou::*"
  }
   ]
  }
```

4. Enterprise account CompanyExampleA of Company A (with ownerUin as 12345) calls AttachRolePolicy to bind the policy created in step 1 to the role DevOpsRole, with policyName=DevOpsPolicy and roleName=DevOpsRole as input parameters.

At this point, Company A's enterprise account CompanyExampleA (ownerUin: 12345) has created a new role and granted permissions to the role.

Creating a role for an identity provider

Before creating a role for an identity provider, you need to create a SAML identity provider in CAM. For information on how to create a SAML identity provider, see Create a SAML Identity Provider.

1. Prepare a trust policy for the role to be created.

> **Note**
> The fields of the trust policy are defined as follows:
> - Action field: Defines the interface that allows SAML federated identities to use the current role. Use `sts:AssumeRoleWithSAML` .
> - Principal field: Defines the identity provider allowed to use the current role. Use the `{"federated": [ IdPArn ]}` string, for example, qcs::cam::uin/10001:saml−provider/idp_name.
> - Condition field: Defines the conditions under which the current role can be used. By default, it uses `{"StringEquals": {"SAML:aud": "https://cloud.tencent.com/login/saml"}}` . This condition restricts the use of this role to identity providers whose SAML federation endpoint is Tencent Cloud.

Below is an example of a role trust policy:

```
    {
  "version": "2.0",
  "statement": [
    {
     "action": "name/sts:AssumeRoleWithSAML",
     "effect": "allow",
     "principal": {
      "federated": [
        "qcs::cam::uin/10001:saml-provider/idp_name"
  ]
     },
     "condition": {
      "string_equal": {
        "saml:aud": "https://cloud.tencent.com/login/saml"
 }
```

```
}
}
 ]
}
```

2. Prepare a permission policy for the role you are about to create. For more information on permission policies, see Policies.
3. Invoke the cam:CreateRole interface to create an identity provider role.

Usage Requirements

SAML currently supports the following conditions:

Condition keys	Description	Required	Note
saml:aud	Recipient	Optional	The URL of the endpoint to which SAML assertion is submitted. The value of this key comes from the `SAML Recipient` rather than `Audience` field in the assertion.
saml:iss	Sender	Optional	This key is represented as a URN. The value of this key comes from the `SAML Issuer` field in the assertion.
saml:sub	External account ID	Optional	This is the subject of the statement, which contains a value uniquely identifying a user within the organization. This key originates from the SAML NameID field in the assertion.
saml:sub_type	External user type	Optional	The value of this key comes from the `Format` attribute in the `SMAL NameID` field in the assertion.

OIDC currently supports the following conditions:

Condition keys	Description	Required	Note
oidc:iss	OIDC issuer	"ActionStatus": "OK",	The constraint must use string_equal, and the condition value can only be the IdP URL you filled in the OIDC identity provider. The iss field value in the OIDC token used to assume the role must meet this constraint requirement for the role to be assumed.
oidc:aud	OIDC audience	"ActionStatus": "OK",	This condition must use string_equal, and the condition value can only use one or more client IDs configured in the OIDC identity provider. The aud field value in the OIDC token used to assume the role must meet this condition requirement for the role to be assumed.
oidc:sub	OIDC subject	Optional	This constraint can utilize any string class condition operation type, and the condition value can set up to 10 OIDC principals. The role can only be assumed when the 'sub' field value in the OIDC token used for role impersonation meets this constraint requirement.

Modifying Role

Last updated：2023-08-31 17:30:45

Scenario

This document outlines the process of editing and modifying the associated policy and role entity of a role. Upon successful modification, the role will manage the resources under the primary account within the scope of the permissions obtained based on the current settings.

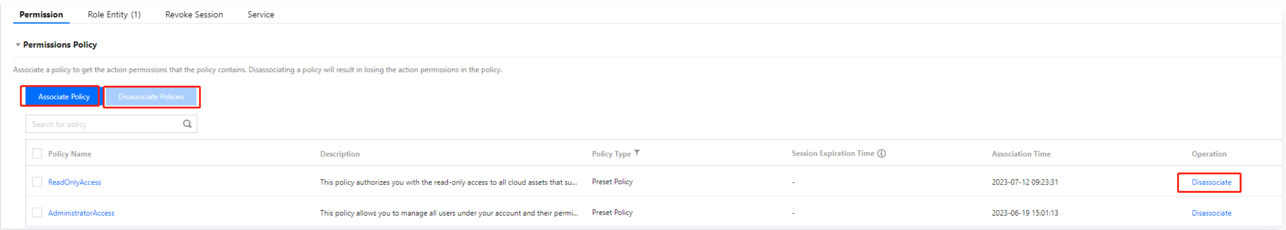
Preparations

You have logged into the Cloud Access Management Console and navigated to the Roles list page.

Instructions

Editing policies associated with a role

1. On the Roles page, click the name of the role you want to modify to go to the role details page.
2. In the **Permission** > **Permissions Policy** section of the Role Details page, you can associate or disassociate policies with the role.



▾ Permissions Policy

Associate a policy to get the action permissions that the policy contains. Disassociating a policy will result in losing the action permissions in the policy.

□ Policy Name	Description	Policy Type	Session Expiration Time	Association Time	Operation
□ ReadOnlyAccess	This policy authorizes you with the read-only access to all cloud assets that su...	Preset Policy	-	2023-07-12 09:23:31	Disassociate
□ AdministratorAccess	This policy allows you to manage all users under your account and their permi...	Preset Policy	-	2023-06-19 15:01:13	Disassociate

Associate Policy

1. Click **Associate Policy**.
2. Select the policies you want to add to the current role from the policy list.
3. Click **OK** to finalize the editing of the associated role operation.

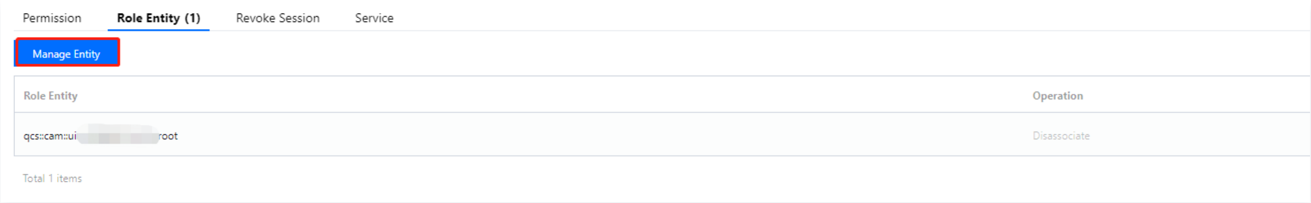
Disassociate Policy

1. In the policy list, click **Disassociate** in the operation column.
2. In the pop-up window for disassociating policies, click **Confirm Disassociation** to disassociate the current policy from the role.

> **Note**
> You can also select multiple policies and click **Disassociate Policies** to disassociate multiple policies.

Editing the role entity

1. On the Roles page, click the name of the role you want to modify to go to the role details page.
2. On the Role Details page, click **Role Entity** to access the Role Entity operation bar.
3. Click on **Manage Entity** to enter the Role Entity Settings page.



Role Entity	Operation
qcs::cam::ui[redacted]root	Disassociate

Total 1 items

4. On the Role Entity page, you can modify the following information according to your needs:
    - For account modifications: Click **Add Account** to add a primary account as the role entity for the current role, or delete the corresponding account tag to remove it from the role entity.
    - For service modifications: Click **Add Product Service**. In the pop-up window, select the product service to be the role entity for the current role, or deselect the corresponding product service to remove it from the role entity.
5. Click **Update** to complete the editing of the role entity.

Using Role

Last updated：2024-01-26 16:03:16

Scenario

You can use roles through the console or APIs. This document describes how to use roles with typical examples.

Preparations

Suppose that:

- Company A has outsourced an operations engineer position to Company B and wishes this role to have access to all CVM resources in the Guangzhou region of Company A.
- It is known that the ownerUin of the corporate account CompanyExampleA of Company A is 12345.
- It is known that the ownerUin of the corporate account CompanyExampleB of Company B is 67890.
- Company B has a sub-account, DevB, who is expected to carry out this task.

Instructions

You can click the following tabs to view the corresponding directions.

Use Roles through the Console

1. Company A creates a role for Company B (see Create Role).
   Select **Tencent Cloud Account** as the role entity to create a role, such as DevOpsRole, set the role entity as Company B's corporate account "67890", and attach permissions to the DevOpsRole role that can operate all CVM resources in the Guangzhou region of Company A.
2. Company B authorizes its sub-account (see Grant Sub-account the Policy to Assume a Role). To grant the sub-account DevB of Company B the policy to assume the DevOpsRole role of Company A (ownerUin is 12345), the policy must include the "sts:AssumeRole" API permission.

   > **Note**
   > Currently, the primary account does not support switching roles in the console. You need to authorize the role for the sub-account under the primary account that carries the role.

3. The sub-account of Company B logs in to the console using a role.
   The sub-account DevB of Company B logs in to the console, selects "Switch Role" from the dropdown menu under the console avatar, and enters the Switch Role page.
   Input the primary account "12345" of Company A and the role name "DevOpsRole". After confirming, they switch to the DevOpsRole role of Company A (ownerUin is 12345).
   If there is a need to switch to other roles, they can select "Switch Role" from the dropdown menu under the console avatar and switch to other roles on the Switch Role page.
   After logging in by switching roles in the console, if you want to return to the original sub-user, you can select "Return to Sub-user" from the dropdown menu under the console avatar to exit the role and return to the original sub-user.

   > **Note**
   > You can only switch to a role after being authorized to use it, and the role entity must be a Tencent Cloud account. You cannot switch to unauthorized roles.

Use Roles through API

Company A, seeing the Create via API document, performs the following operations:

1. Create a role, and set the role entity to Company B’s enterprise account, `CompanyExampleB`.
2. Call the `CreateRole` API to create a role with the `roleName` as `DevOpsRole`, and grant the role the permissions allowing it to

operate all Company A’ s CVM resources in the Guangzhou region.

Company B, seeing the Assign Role Play Policy to a Sub-account document, performs the following actions:

1. Authorize the sub-account `DevB` to assume the `DevOpsRole` role.
2. Invoke the AssumeRole API to request temporary credentials for the DevOpsRole role. The input parameters are as follows:

   > **Note**
   > If company B (`CompanyExampleB`) wants to directly operate the resources of company A (`CompanyExampleA`), they can also request temporary credentials to perform operations.

   ```
   roleArn=qcs::cam::uin/12345:roleName/DevOpsRole,
   roleSessionName=DevBAssumeTheRole,
   durationSeconds=7200
   ```

   If this API is called successfully, the response will be as follows:

   ```
   {
     "credentials": {
       "sessionToken": "5e776c4216ff4d31a7c74fe194a978a3ff2a42864",
       "tmpSecretId": "AKI*PCI",
       "tmpSecretKey": "Vpx*MqD"
     },
     "expiredTime": 1506433269,
     "expiration": "2018-09-26T13:41:09Z"
   }
   ```

3. Within the validity period of the credentials, DevB performs operations within the scope of Company A's permissions as needed. For instance, when calling the DescribeInstances API to view the list of CVMs, replace the values of the API keys SecretId and SecretKey with the values of tmpSecretId and tmpSecretKey, and set the Token in Common Parameters to the value of sessionToken.

   > **Note**
   > When Company A wishes to revoke the authorization to Company B, it can simply delete the role DevOpsRole.

Deleting a Role

Last updated：2023-08-31 17:32:18

Scenario

This document outlines the process of deleting a role. Once deleted, the role will no longer have access to manage resources under the primary account's authority.

Instructions

1. Log in to the Cloud Access Management (CAM) console and navigate to the Roles list page.
2. In the Roles page, select the role you want to delete.
3. Click on **Delete** in the operations column, then **Confirm** to complete the role deletion process.

> **Note**
> Deleting a role will also remove the authorization information associated with it. The product services or accounts that act as the role entity for this role will no longer be able to use it.

Authorizing Sub-account with Role Assuming Policy

Last updated：2024-01-26 16:05:37

A root account as the entity of a role can allow its sub-accounts to assume the role. The following example shows how to create and assign policies for role assumption.

For example, Company A wants to outsource its Ops Engineer position to Company B. The person taking the position needs the access to all Company A's CVM resources located in the Guangzhou region.

Company A's corporate account, CompanyExampleA (with primary account ID 12345), creates a role and sets the entity of the role as Company B's corporate account, CompanyExampleB (with primary account ID 67890). Company A (CompanyExampleA) calls the CreateRole interface to create a role named DevOpsRole and attaches permissions to the created role. For more information on these steps, see Creation via API.

After being authorized with this role, Company B's corporate account (CompanyExampleB) wants its sub-account, DevB, to perform the tasks. Company B (CompanyExampleB) needs to grant permission to its sub-account DevB to assume the role of DevOpsRole from Company A (CompanyExampleA):

1. Under Company B's corporate account, CompanyExampleB (with primary account ID 67890), create a policy named AssumeRole. Here is an example:

```
{
 "version": "2.0",
 "statement": [
 {
    "effect": "allow",
    "action": ["name/sts:AssumeRole"],
    "resource": ["qcs::cam::uin/12345:roleName/DevOpsRole"]
 }
 ]
}
```

2. Assign this policy to the sub-account DevB. The sub-account is thus granted the permission to assume the role of DevOpsRole.
3. For information on how to use the role after the sub-account has been granted the permission to assume the role, see Using Roles.

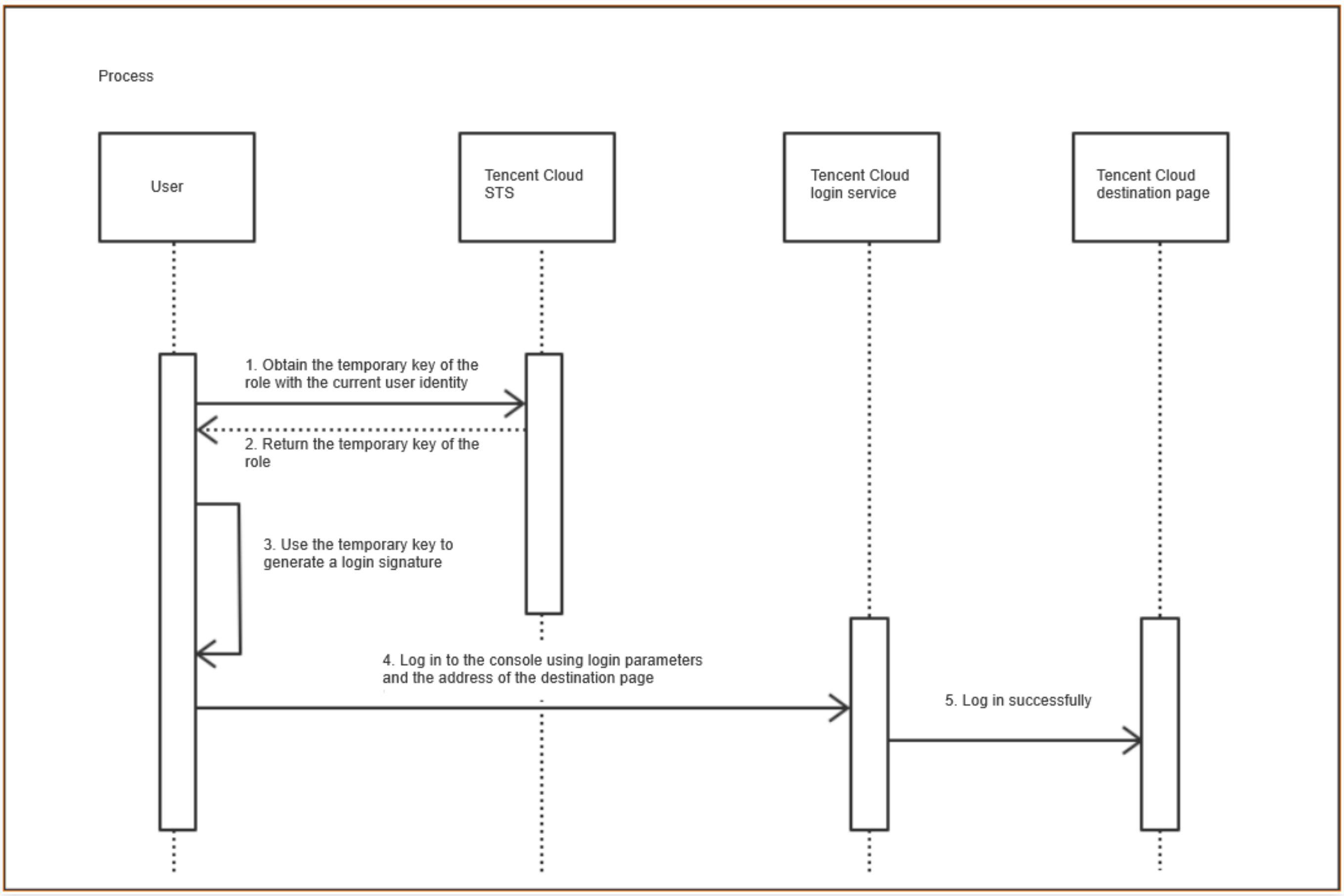
Password-Free Login to the Console via Role

Last updated：2024-01-26 16:08:14

Scenario

This document outlines the detailed process of implementing password-free login to the console through role identity. A typical scenario is: After you have configured the Tencent Cloud Log Service for collection and query analysis, you expect to directly access the analysis content of the log service without needing to log in to the Tencent Cloud Log Service console. After configuring according to this document, you can log in to the third-party site to use the Tencent Cloud embedded console page.

Operations Guide


Process
User
Tencent Cloud STS
Tencent Cloud login service
Tencent Cloud destination page
1. Obtain the temporary key of the role with the current user identity
2. Return the temporary key of the role
3. Use the temporary key to generate a login signature
4. Log in to the console using login parameters and the address of the destination page
5. Log in successfully

Preparations

1. You need to create a role with an account as the role carrier, and allow it to log in to the console. In this document, this role is assumed to be named MyRole. For creating a role, please refer to Create Role - API Documentation.
2. Obtain the current user's access key. For information on how to obtain a persistent key, see Access Key for Current User.

Instructions

> **Note**
> There may be potential risks in the settings. Please operate in accordance with the security recommendations:
> - The validity period of the temporary key should not be set too long. It is recommended that you set it within 5 minutes, which can be specified by calling AssumeRole and through the DurationSeconds parameter.
> - Please do not expose the complete login address containing parameters (`https://cloud.tencent.com/login/roleAccessCallback?algorithm...`) on the public network.
> - The system used by the user to generate login addresses needs to be set with authentication, such as internal network identity verification. Please do not set it to public access.

1. Users use the access key obtained in Precondition 2 to call the AssumeRole interface, applying for the temporary key of the role MyRole that was pre-created in Precondition 1.
2. After successfully calling the AssumeRole interface, the user obtains the temporary key for the role MyRole.
3. Users generate login signature information through the temporary key of this role. For details, please see the following steps:

3.1 **Parameter Sorting**: The parameters requiring signature are sorted in ascending order according to the alphabet or numerical table. The first letter is considered first, and the second letter is considered in the same situation, and so on. You can use the relevant sorting functions in programming languages to achieve this function, such as the ksort function in PHP. The signature parameters include the following content:

Parameter name	Required	Type	Description
action	Supported	String	Action; fixed as `roleLogin`
timestamp	Supported	Int	Current timestamp
nonce	Supported	Int	Random integer, value between 10,000 and 100,000,000.
secretId	Supported	String	Temporary AK returned by STS

3.2 **Concatenate Parameters**: The sorted request parameters from the previous step are concatenated in the format "parameter name=parameter value". For example:

```
action=roleLogin&nonce=67439&secretId=AKI*PLE&timestamp=1484793352
```

3.3 **Concatenate Signature String**: Concatenate the signature string according to the rule of `Request Method + Request Host + Request Path + ? + Request String`.

Category	Required	Description
Request CVM and path	Supported	Set to cloud.tencent.com/login/roleAccessCallback
Request method	Supported	Supports GET or POST

Signature string example:

```
GETcloud.tencent.com/login/roleAccessCallback?
action=roleLogin&nonce=67439&secretId=AKI*PLE&timestamp=1484793352
```

3.4 **Generate Signature String**: Sign the string using the HMAC-SHA1 algorithm, currently supporting HMAC-SHA1 and HMAC-SHA256. The specific code is as follows, using PHP as an example:

```
$secretKey = 'Gu5*1qA';
$srcStr    = 'GETcloud.tencent.com/login/roleAccessCallback?
action=roleLogin&nonce=67439&secretId=&timestamp=1484793352';
$signStr   = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

PHP Version Sample Code:

```
<?php
$secretId  = "AKI*";           //Temporary AK returned by STS
$secretKey = "Gu5*PLE";        //Temporary Secret returned by STS
$token     = "ADE*fds";        //Security TOKEN returned by STS
$param["nonce"]     = 11886;     //rand();
$param["timestamp"] = 1465185768; //time();
$param["secretId"]  = $secretId;
$param["action"]    = "roleLogin";
ksort($param);
```

```
$signStr = "GETcloud.tencent.com/login/roleAccessCallback?";
foreach ( $param as $key => $value ) {
        $signStr = $signStr . $key . "=" . $value . "&";
}
$signStr   = substr($signStr, 0, -1);
$signature = base64_encode(hash_hmac("sha1", $signStr, $secretKey, true));
echo $signature.PHP_EOL;
```

4. Concatenate the complete login information and the destination page address for login. The **parameter values need to be urlencode encoded**.

```
https://cloud.tencent.com/login/roleAccessCallback
        ?algorithm=<Encryption algorithm used during signing, currently only supports sha1 and sha256, if not filled, sha1 is
the default>
        &secretId=<SecretId used during signing>
        &token=<Temporary key token>
        &nonce=<nonce at the time of signing>
        &timestamp=<timestamp at the time of signing>
        &signature=<Signature String>
        &s_url=<Destination URL after login>
```

5. After Tencent Cloud Login Service verifies the login information correctly, it redirects to the Tencent Cloud destination page.

Resource-Based Service Role

Last updated：2024-01-26 16:09:42

Scenario

A role is a virtual identity with a set of permissions. It is used to grant access permissions to services, operations, and resources in Tencent Cloud for role entities. You can associate roles with cloud resources and access APIs of other cloud products within cloud resources based on the STS temporary keys of Tencent Cloud Security Credential Service (the temporary keys can be updated periodically). Compared with direct permission control using persistent keys, this method can further ensure the security of persistent keys under the account and implement more refined control and permission management based on role association policies.

Strengths

Upon binding a CAM role to cloud resources, the following features and advantages will be available:

- You can access other Tencent Cloud services using STS temporary keys. For more information, see STS APIs.
- You can assign roles with different authorization policies to different resources, enabling cloud resources to have different access permissions to different cloud services, thereby achieving more granular permission control.
- There is no need to save persistent keys in instances by yourself. You can modify the permissions of a role to change the access permissions of users or services to cloud resources, quickly maintaining cloud resource permissions.

Instructions

If you need to bind a role to your Tencent Kubernetes Engine (TKE) - Container Instance, please see Bind a Role to a Container Instance.
If you need to bind a role to your Serverless Cloud Function (SCF) - Function Service, please see Roles and Policies - Configuring Roles.
If you need to bind a role to your Cloud Virtual Machine (CVM) - Cloud Server, please see Managing Instance Roles.

Identity Provider

SSO Overview

Last updated：2024-01-26 17:22:17

Tencent Cloud supports SAML 2.0 and OIDC-based Single Sign-On (SSO), allowing external users authenticated by your IdP to directly access your Tencent Cloud resources. Currently, Tencent Cloud offers two SSO login methods: User-Based SSO and Role-Based SSO.

Fundamental Concepts of SSO

Concept	Note
IdP	An entity that contains metadata about an external IdP, which can offer identity management services. • Enterprise Local IdP: Microsoft Active Directory Federation Service (ADFS), Shibboleth, etc. • Cloud IdP: Azure AD, Google Workspace, Okta, OneLogin, etc.
Service Provider (SP)	Leveraging the identity management capabilities of the IdP, the SP utilizes the user information provided by the IdP to offer specific services. Some non-SAML protocol identity systems, such as OpenID Connect, also see the SP as a trusted party of the IdP.
Security Assertion Markup Language (SAML 2.0)	SAML 2.0 is a standard protocol for enterprise-level user authentication, serving as one of the technical implementations for communication between SP and IdP. It has become a de facto standard for implementing enterprise-level SSO.
SAML Assertion	The core element in the SAML protocol used to describe authentication requests and responses. For instance, specific user attributes are included in the assertions of the authentication response.
Trust	A trust mechanism established between the SP and IdP, typically implemented using public and private keys. The SP obtains the IdP's SAML metadata in a trusted manner, which includes the public key for verifying the signature of the SAML assertion issued by the IdP. The SP uses this public key to verify the integrity of the assertion.
OIDC	OIDC (OpenID Connect) is an authentication protocol built on the foundation of OAuth 2.0. OAuth is an authorization protocol, while OIDC builds an identity layer on top of the OAuth protocol. In addition to the authorization capabilities provided by OAuth, it also allows clients to verify the identity of end users and obtain basic user information through the API of the OIDC protocol (in the form of HTTP RESTful).
OIDC Token	OIDC can issue identity tokens representing logged-in users, known as OIDC Tokens. These tokens are used to obtain basic information about the logged-in user.
The client ID	When your application registers with an external IdP, a Client ID is generated. This Client ID is required when requesting the issuance of an OIDC token from the external IdP, and the issued OIDC token will carry this Client ID in the 'aud' field. When creating an OIDC identity provider, configure this Client ID. Then, when using the OIDC token to exchange for an STS Token, Tencent Cloud will verify whether the Client ID carried in the 'aud' field of the OIDC token matches the Client ID configured in the OIDC identity provider. Role assumption is only permitted if they match.
Verify fingerprint	To prevent the issuer URL from being maliciously hijacked or tampered with, you need to configure the verification fingerprint generated by the external IdP's HTTPS CA certificate. Tencent Cloud will assist you in automatically calculating this verification fingerprint, but it is recommended that you calculate it locally (for example, using OpenSSL to calculate the fingerprint) and compare it with the fingerprint calculated by Tencent Cloud. If the comparison reveals differences, it indicates that the issuer URL may have been attacked. Please make sure to confirm again and fill in the correct fingerprint.

IdP URL	The identifier for the OpenID Connect IdP. This corresponds to the "issuer" field value in the OpenID Connect metadata document provided by the IdP.
map fields	The field in the OpenID Connect IdP that maps to the Tencent Cloud CAM sub-user name. You can choose from the "claims_supported" values in the OpenID Connect metadata document provided by the IdP. In this example, the 'name' field maps to the CAM 'username'.
Public Key for Signature	The public key used to verify the ID Token signature of the OpenID Connect IdP. This corresponds to the content linked in the "jwks_uri" field of the OpenID Connect metadata document provided by the IdP (the content can be obtained by opening the link in a browser). For the safety of your account, it is recommended to periodically rotate your signature public key.

Through SSO

Tencent Cloud offers the following two SSO methods:

User-Based SSO

Tencent Cloud determines the correspondence between enterprise users and Tencent Cloud CAM users through the SAML assertion issued by the IdP. Enterprises can manage employee information in the local IdP without needing to synchronize users between Tencent Cloud and the enterprise IdP. Enterprise employees can log in to Tencent Cloud through specified CAM roles. After the enterprise user logs in, they can access Tencent Cloud resources using that CAM user. For more information, please refer to User SSO Overview.

Role-Based SSO

Tencent Cloud determines the correspondence between enterprise users and Tencent Cloud CAM users through the SAML assertion or OIDC token issued by the IdP. Once the enterprise users are logged in, they can access Tencent Cloud using the corresponding CAM user. Tencent Cloud supports two types of Role-Based SSO: SAML 2.0-based and OIDC-based.

- SAML Role-Based SSO: Tencent Cloud determines the CAM roles that enterprise users can use on Tencent Cloud based on the SAML assertion issued by the IdP. After logging in, enterprise users access Tencent Cloud resources using the CAM roles specified in the SAML assertion. For more information, see SAML Role-Based SSO Overview.
- OIDC Role-Based SSO: Enterprise users, through the OIDC token issued by the IdP, invoke Tencent Cloud API to impersonate a specified role and exchange it for a temporary STS token. This STS token is then used to securely access Tencent Cloud resources. For more information, see OIDC Role-Based SSO Overview.

Comparison of SSO Methods

Through SSO	SP-Initiated SSO	IdP-Initiated SSO	Logging in using the sub-account's username and password	One-time configuration of IdP to associate multiple Tencent Cloud accounts	Multiple IdPs
User-Based SSO	This feature is supported.	This feature is supported.	Unavailable	Unavailable	Unavailable
Role-Based SSO	Unavailable	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.

Applicable Scenarios for SSO

Last updated：2024-01-26 17:23:07

Tencent Cloud currently supports two SSO methods: Role-Based SSO and User-Based SSO. This document will guide you through the applicable scenarios and selection criteria for these two methods, assisting you in choosing the appropriate SSO method based on your overall business requirements.

Role-Based SSO

The following scenarios are suitable for Role-Based SSO:

- To reduce management costs, you prefer not to create and manage users in the cloud, thereby avoiding the workload brought about by user synchronization.
- While utilizing SSO, you wish to retain some local users in the cloud who can directly log in to Tencent Cloud. These local users can serve various purposes, such as testing new features or acting as an alternative login method in case of network or enterprise IdP issues.
- You wish to differentiate the permissions held in the cloud based on the group a user joins in the local IdP or a particular attribute of the user. When adjusting permissions, you only need to make changes to the group or attribute locally.
- You have multiple Tencent Cloud accounts but use a unified enterprise IdP. You wish to configure the enterprise IdP once and achieve SSO for multiple Tencent Cloud accounts.
- Your various branches have multiple IdPs, all of which need to access the same Tencent Cloud account. You need to configure multiple IdPs within a single Tencent Cloud account for SSO.
- In addition to the console, you also wish to implement SSO through programmatic access.

User-Based SSO

The following scenarios are suitable for User-Based SSO:

- You prefer initiating the login process from Tencent Cloud's login page, rather than directly accessing your IdP's login page.
- Some of the cloud products you need to use temporarily do not support role-based access. For cloud products that support role-based access (i.e., access via STS), see Business Supporting Roles.
- Your IdP does not support complex custom attribute configurations.
- You do not have the above-mentioned business requirements for using Role-Based SSO, but you still wish to simplify the IdP configuration as much as possible.

User SSO

Overview of User-Based SSO

Last updated：2024-01-26 17:25:55

Scenario

When Tencent Cloud and an enterprise implement user SSO, Tencent Cloud acts as the Service Provider (SP), while the enterprise's own identity management system serves as the IdP. Through user SSO, once enterprise employees log in, they access Tencent Cloud as CAM sub-users.

Instructions

Configuration Workflow

Before implementing user-based SSO, you must establish trust between Tencent Cloud and your IdP by configuring Security Assertion Markup Language (SAML) on both sides.

1. Configure your IdP to Tencent Cloud.
   - Objective: To establish trust between Tencent Cloud and your enterprise's IdP.
   - For specific configuration steps, see Configure SAML for Tencent Cloud SP.
2. Configure Tencent Cloud as a trusted SP in your IdP and configure the SAML assertion attributes.
   - Objective: To establish trust from the enterprise IdP towards Tencent Cloud.
   - For specific configuration steps, see Configuring SAML for Enterprise IdP.
3. Enterprises log in to the Cloud Access Management Console or create a CAM sub-user via API call that perfectly matches the name in the enterprise IdP.
   - Objective: To utilize sub-users for subsequent login operations.
   - For detailed configuration operations, see Create a Sub-User.

Login and verification process

Upon completion of the aforementioned user SSO configurations, users in the enterprise IdP can log in to Tencent Cloud via SSO and access authorized resources. For instance, the specific login verification process for a user named 'user1' would be as follows:

1. "user1" initiates user-based SSO login on the sub-user login page.
2. Tencent Cloud returns an SAML assertion authentication request to the browser.
3. The browser forwards the SAML authentication request to the IdP.
4. The IdP authenticates user1 and returns the generated SAML response to the browser after the authentication is passed.
5. The browser forwards the SAML response to Tencent Cloud.
6. Tencent Cloud verifies the authenticity and integrity of the SAML assertion based on the SAML mutual trust configuration and then maps the value of the `NameID` element in the SAML assertion to the CAM sub-user.
7. After successful verification and mapping, Tencent Cloud returns the URL of Tencent Cloud console to the browser, and user1 can log in to the console successfully.

Configuring OIDC In Tencent Cloud SP

Last updated：2024-01-26 17:28:29

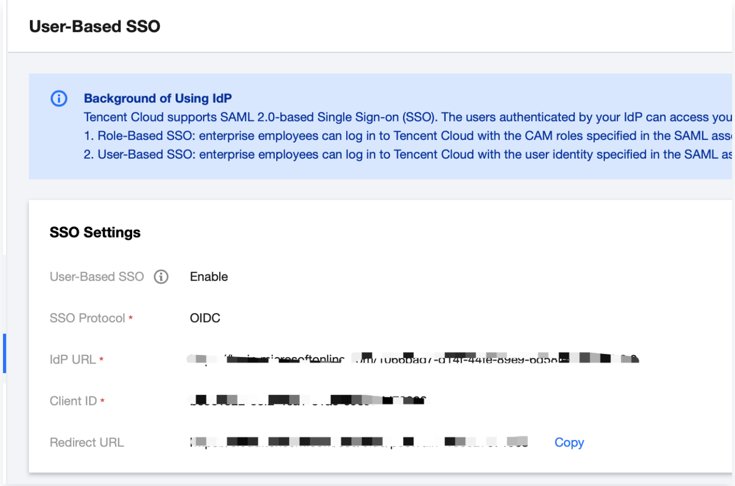
Scenario

As a Service Provider (SP), Tencent Cloud needs to configure the OpenID Connect (OIDC) for the enterprise Identity Provider (IdP) to establish trust with the enterprise IdP. This allows enterprise IdP users to log in to Tencent Cloud using User Single Sign-On (SSO). This document uses Azure Active Directory as an example of an IdP.

> **Note**
> View the OIDC protocol configuration information. (Copy the link from Azure Active Directory > App registrations > Endpoints > OpenID Connect metadata document, and open it in a browser to obtain the specific configuration information.)

Instructions

1. Log in to the Cloud Access Management Console with your Tencent Cloud account.
2. In the left sidebar, click on **Identity Provider** > **User SSO**.
3. On the User-Based SSO page, you can view the User-Based SSO status and the configuration information.



User-Based SSO

Background of Using IdP
Tencent Cloud supports SAML 2.0-based Single Sign-on (SSO). The users authenticated by your IdP can access you
1. Role-Based SSO: enterprise employees can log in to Tencent Cloud with the CAM roles specified in the SAML ass
2. User-Based SSO: enterprise employees can log in to Tencent Cloud with the user identity specified in the SAML as

SSO Settings

User-Based SSO: Enable

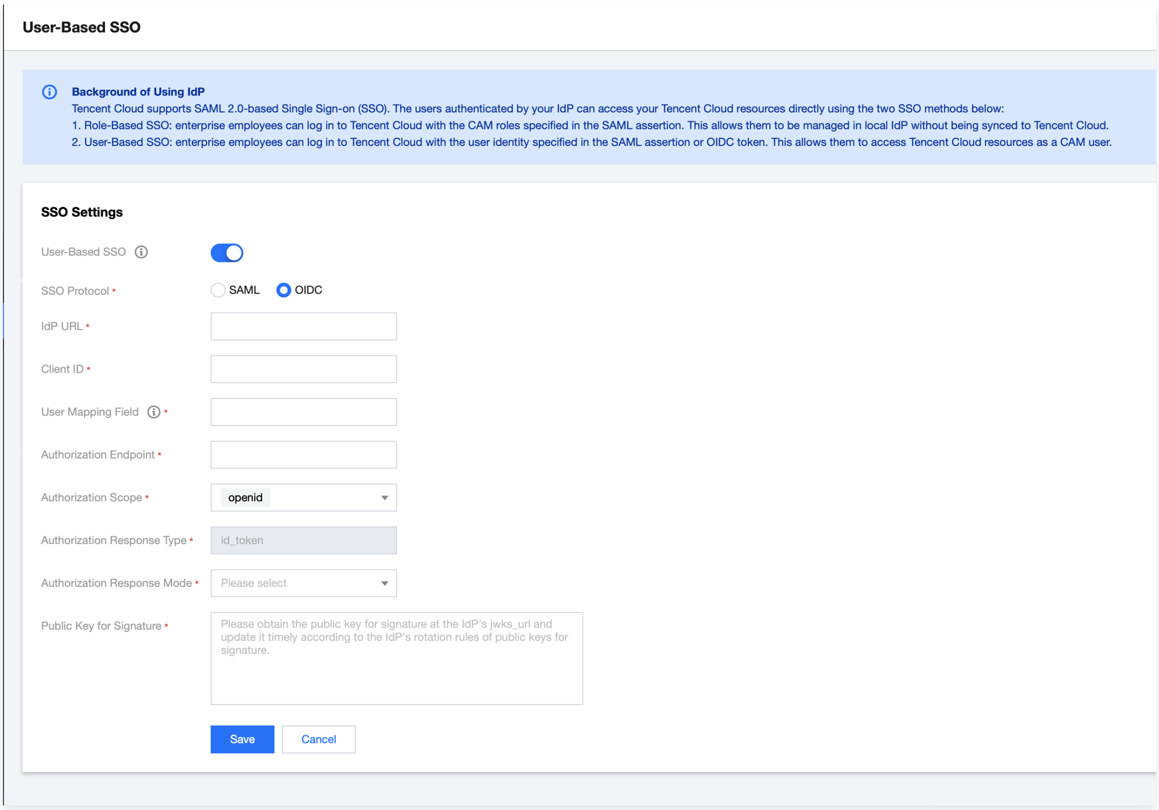
SSO Protocol *: OIDC

IdP URL *: [redacted]

Client ID *: [redacted]

Redirect URL: [redacted] Copy

4. You can enable or disable User-Based SSO by clicking on the button next to it.



User-Based SSO

Background of Using IdP
Tencent Cloud supports SAML 2.0-based Single Sign-on (SSO). The users authenticated by your IdP can access your Tencent Cloud resources directly using the two SSO methods below:
1. Role-Based SSO: enterprise employees can log in to Tencent Cloud with the CAM roles specified in the SAML assertion. This allows them to be managed in local IdP without being synced to Tencent Cloud.
2. User-Based SSO: enterprise employees can log in to Tencent Cloud with the user identity specified in the SAML assertion or OIDC token. This allows them to access Tencent Cloud resources as a CAM user.

SSO Settings

User-Based SSO: on
SSO Protocol *: ○ SAML ● OIDC
IdP URL *
Client ID *
User Mapping Field *
Authorization Endpoint *
Authorization Scope *: openid
Authorization Response Type *: id_token
Authorization Response Mode *: Please select
Public Key for Signature *: Please obtain the public key for signature at the IdP's jwks_url and update it timely according to the IdP's rotation rules of public keys for signature.

- When enabled, CAM sub-users cannot log in to Tencent Cloud using their account passwords. Instead, all CAM sub-users are redirected to the enterprise IdP login page for identity authentication.
- When disabled, CAM sub-users can log in to Tencent Cloud using their account credentials, and the User SSO settings will not take effect.
- SSO Protocol: Select the OIDC type.
- IdP URL: The identifier for the OpenID Connect IdP. This corresponds to the "issuer" field value in the OpenID Connect metadata document provided by the IdP.
- Client ID: The client ID registered with the OpenID Connect IdP. This can be obtained from the **Azure Active Directory > Enterprise Applications > OIDCSSO Application Overview page**.
- User Mapping Field: The field in the OpenID Connect IdP that maps to the Tencent Cloud CAM sub-user name. You can choose the value of "claims_supported" in the OpenID Connect metadata document provided by the IdP. In this example, the 'name' field is used to map the CAM 'username'.
- Authorization Request Endpoint: This is the authorization request address of the OpenID Connect IdP. It corresponds to the "authorization_endpoint" field value in the OpenID Connect metadata document provided by the IdP.
- Authorization Request Scope: The scope of authorization request information for the OpenID Connect IdP. The default and required selection is openid.
- Authorization Request Response type: The return parameter type of the OpenID Connect IdP authorization request. By default, id_token is required.
- Authorization Request Response Mode: The return mode for the OpenID Connect IdP authorization request. You can choose between form_post and fragment modes. It is recommended to select the form_post mode.
- Signature Public Key: The public key used to verify the signature of the OpenID Connect IdP's ID Token. This corresponds to the content of the link in the "jwks_uri" field in the OpenID Connect metadata document provided by the IdP (open the link in a browser to obtain the content). For the security of your account, it is recommended that you rotate the signature public key regularly.

5. Click **Save**.

Configuring SAML In the Enterprise IdP

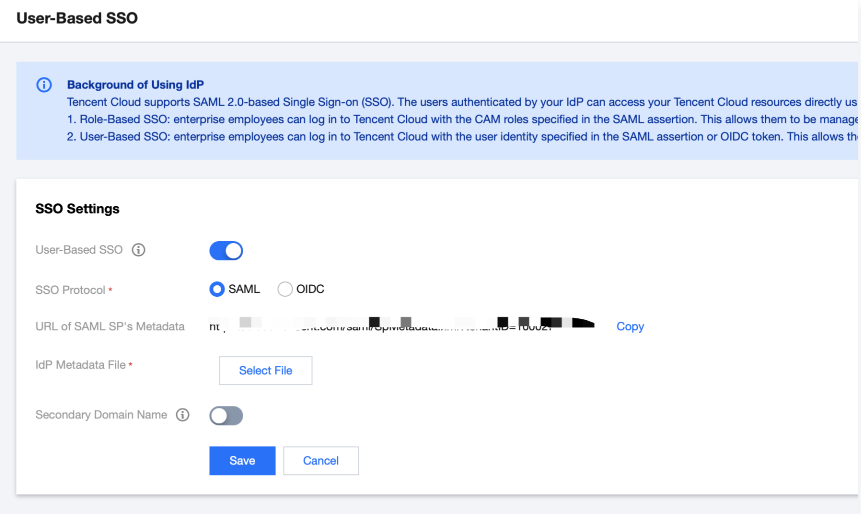
Last updated：2024-01-26 17:41:20

Scenario

The existing identity system of an enterprise acts as an Identity Provider (IdP) and needs to configure SAML for Tencent Cloud Service Provider (SP) to establish trust from the enterprise IdP to Tencent Cloud. This enables enterprise IdP users to log in to Tencent Cloud using User Single Sign-On (SSO).

Instructions

1. Obtain the URL of SAML SP's metadata from Tencent Cloud.
   1.1 Log in to the Cloud Access Management Console with your Tencent Cloud account.
   1.2 In the left sidebar, click **Identity Providers** > **User SSO**.
   1.3 On the User-Based SSO page, you can view or copy the SAML Service Provider metadata URL of the current user.



User-Based SSO

Background of Using IdP
Tencent Cloud supports SAML 2.0-based Single Sign-on (SSO). The users authenticated by your IdP can access your Tencent Cloud resources directly us
1. Role-Based SSO: enterprise employees can log in to Tencent Cloud with the CAM roles specified in the SAML assertion. This allows them to be manage
2. User-Based SSO: enterprise employees can log in to Tencent Cloud with the user identity specified in the SAML assertion or OIDC token. This allows th

SSO Settings

User-Based SSO: on
SSO Protocol *: ● SAML ○ OIDC
URL of SAML SP's Metadata: [redacted] Copy
IdP Metadata File *: Select File
Secondary Domain Name: off

2. Create a SAML SP in your enterprise IdP and configure Tencent Cloud as a trusted SP. The specific configuration method can be chosen from the following options based on the actual situation of your enterprise IdP:
   - If the enterprise IdP supports URL configuration: Copy the URL of Tencent Cloud SP's metadata obtained in step 1 directly into the enterprise IdP for configuration.
   - If your enterprise IdP supports file configuration: Copy the URL of Tencent Cloud SP's metadata from step 1, open it in a browser and save it as an XML file. Then, upload this file to your enterprise IdP for configuration.
   - If the enterprise IdP does not support the above two methods, the following parameters need to be manually configured on the enterprise IdP:

Category	Required or Not	Note
Entity ID	Required or Not	In the downloaded metadata XML, the value of the entityID attribute of the EntityDescriptor element.
ACS URL	Required or Not	In the downloaded metadata XML, the value of the Location attribute of the AssertionConsumerService element.

> **Note**
> If you need to specify a different Tencent Cloud page to redirect to, you can specify it using the format https://cloud.tencent.com/login/saml?s_url=xxxx, where xxxx is the address you need to specify, which needs to be URL-encoded.

Configure OIDC In the Enterprise IdP

Last updated：2024-01-26 17:42:49

Operational Scenario

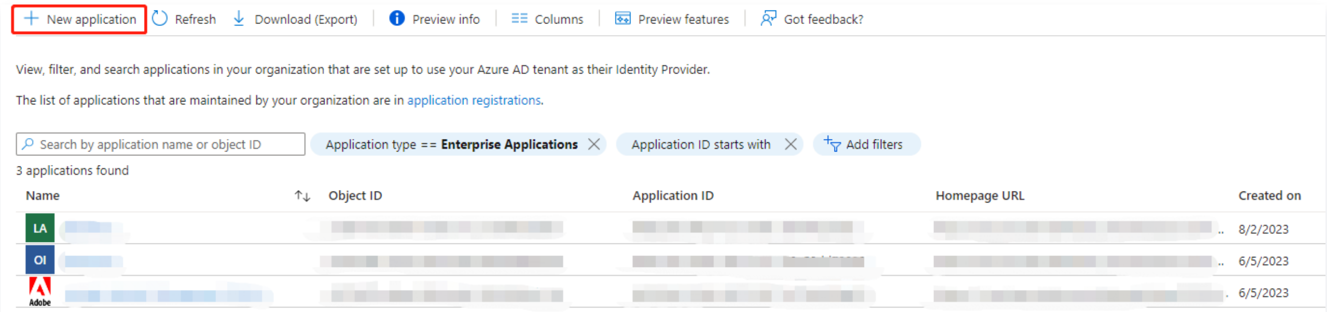
The existing identity system of the enterprise acts as the Identity Provider (IdP) and needs to configure the Tencent Cloud Service Provider (SP) with OpenID Connect (OIDC) to establish trust from the enterprise IdP to Tencent Cloud. This enables enterprise IdP users to log in to Tencent Cloud using User Single Sign-On (SSO).

> **Note:** This document uses Azure Active Directory as an example of an IdP.

Operation Steps

Create an application within the enterprise IdP

1. The administrator logs in to the Azure Active Directory portal.
2. Navigate to Azure Active Directory **> Enterprise Applications > All Applications.**
3. Click **New Application.**



+ New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

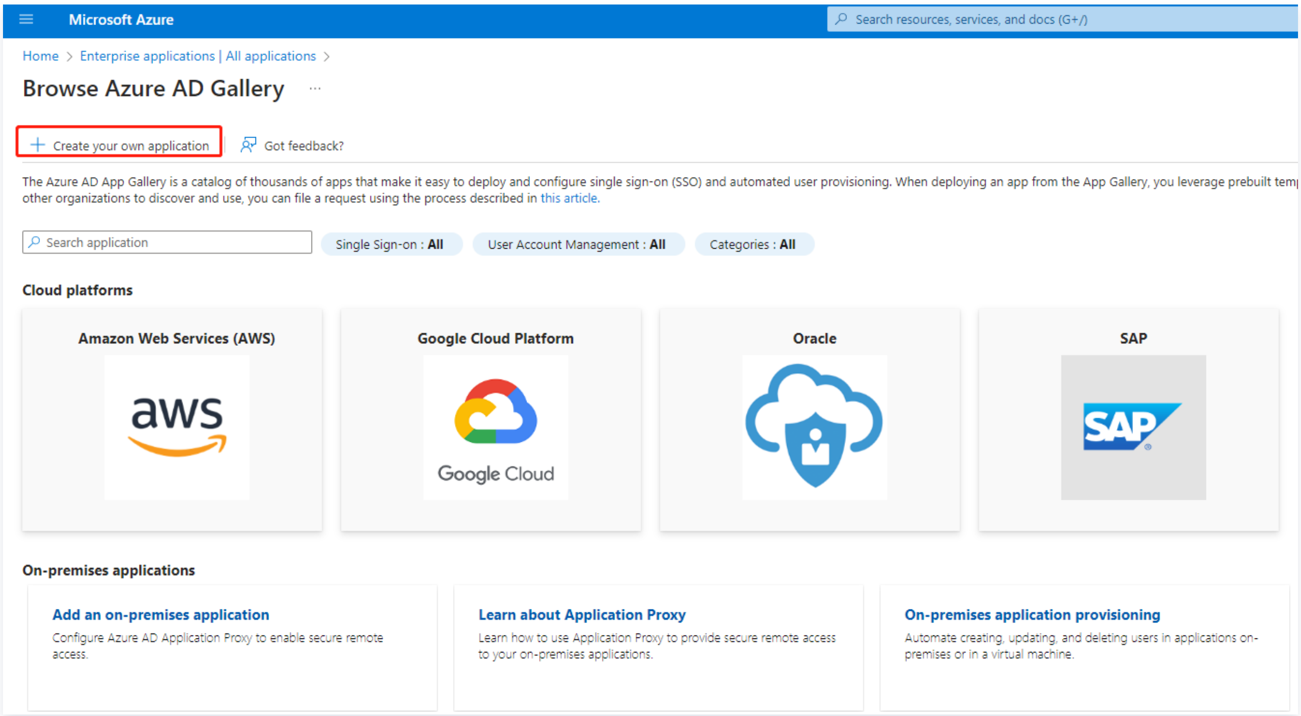
The list of applications that are maintained by your organization are in application registrations.

Search by application name or object ID
Application type == **Enterprise Applications**
Application ID starts with
Add filters

3 applications found

Name	Object ID	Application ID	Homepage URL	Created on
LA [redacted]	[redacted]	[redacted]	[redacted]	8/2/2023
OI [redacted]	[redacted]	[redacted]	[redacted]	6/5/2023
Adobe [redacted]	[redacted]	[redacted]	[redacted]	6/5/2023

4. Click **Create your own application.**



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications | All applications >
Browse Azure AD Gallery
+ Create your own application
Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt temp
other organizations to discover and use, you can file a request using the process described in this article.

Add an on-premises application
Configure Azure AD Application Proxy to enable secure remote access.

Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

On-premises application provisioning
Automate creating, updating, and deleting users in applications on-premises or in a virtual machine.

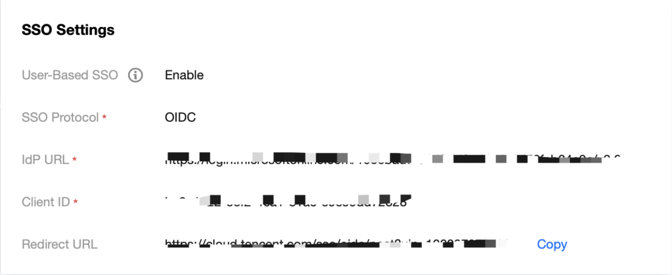
5. In the pop-up window on the right, name your application and select the integration of any other application not found in the library (non-library).

Obtain the OIDC SP metadata URL from Tencent Cloud

1. Log in to the Cloud Access Management Console with your Tencent Cloud account.

> **Note:**
> For Tencent Cloud OIDC configuration, see Configure OIDC for Tencent Cloud SP.

2. Select **Identity Provider** > **User SSO** from the left sidebar. The information is as follows:



SSO Settings

User-Based SSO: Enable

SSO Protocol *: OIDC

IdP URL *: [redacted]

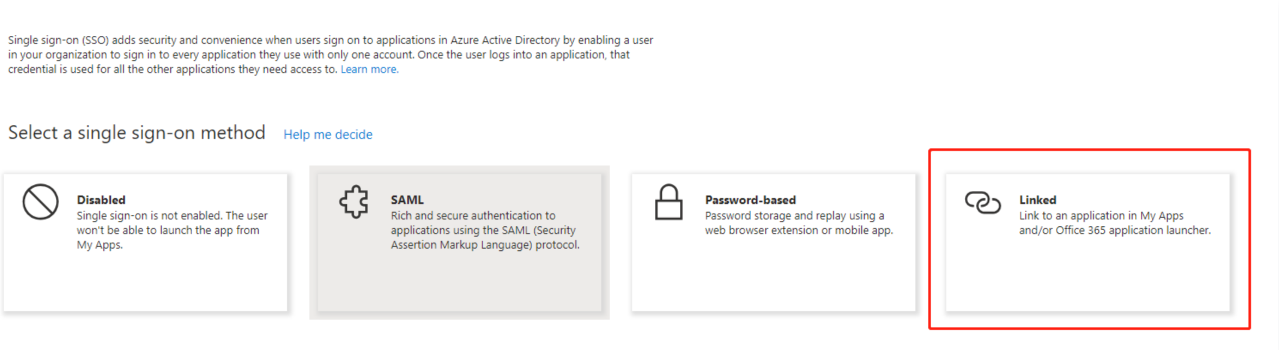
Client ID *: [redacted]

Redirect URL: [redacted] Copy

3. Click **Copy** to retrieve the Redirect URL information.

Enter the Redirect URL obtained from Tencent Cloud into the enterprise IdP

1. Navigate to Azure Active Directory > **App registrations** > **All applications.**
2. Click on the application that has been created in the application name field.
3. On the left sidebar, click **Single Sign-On.**
4. Choose the single sign-on method as a link, as shown in the figure below:



Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method Help me decide

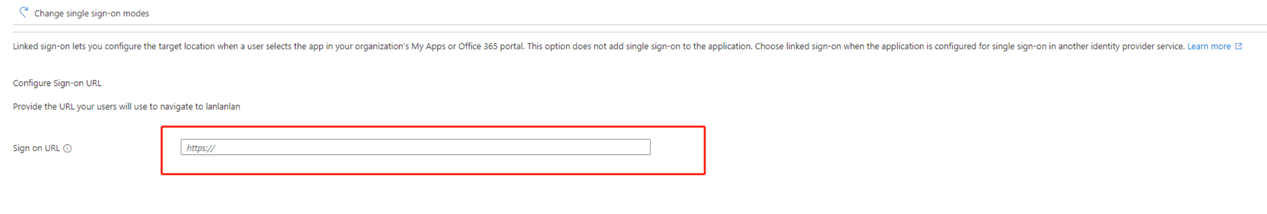
Disabled Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based Password storage and replay using a web browser extension or mobile app.

Linked Link to an application in My Apps and/or Office 365 application launcher.

5. Enter the Redirect URL obtained from Tencent Cloud.



Change single sign-on modes

Linked sign-on lets you configure the target location when a user selects the app in your organization's My Apps or Office 365 portal. This option does not add single sign-on to the application. Choose linked sign-on when the application is configured for single sign-on in another identity provider service. Learn more

Configure Sign-on URL

Provide the URL your users will use to navigate to lanlanlan

Sign on URL: https://

6. Click **Save.**

Role-Based SSO

Overview of Role-Based SSO

Last updated：2024-01-26 17:48:53

If your enterprise or organization already has its own account system and wishes to manage the use of Tencent Cloud resources by its members, Tencent Cloud supports the use of Identity Providers (IdP) so you don't have to create a CAM sub-user for each member within your Tencent Cloud account. Using the IdP service, you can manage Tencent Cloud external user identities, and grant them permissions to use your Tencent Cloud resources.

There is no need for you to customize login code or perform login verification. The IdP provides identity authentication. Once external identity users are authenticated by a known IdP, they log in to Tencent Cloud using a role. You can grant the IdP role permissions to use your Tencent Cloud resources, and external identity users will access resources within the limited permissions of the role. As external identity users log in to Tencent Cloud using a role, and the role uses temporary keys, you can avoid security issues caused by long-term key usage (such as Cloud API keys), which can lead to difficulties in key rotation and potential exposure due to interception.

Use Cases

If your enterprise or organization has established its own account system and users, and these users need to access Tencent Cloud resources, you can use the IdP feature of Tencent Cloud Access Management (CAM) without having to create CAM sub-users for these users in your Tencent Cloud account. By utilizing the IdP feature, you can manage external users of Tencent Cloud and use the role feature to specify Tencent Cloud access permissions for users authenticated by the IdP.

Item

- **No need to create a Tencent Cloud account**
  Enterprise customers do not need to create a Tencent Cloud account for each member of the organization, thereby avoiding security issues caused by the leakage of long-term access certificates (such as Cloud API keys) assigned to users.
- **Federated SSO provision**
  In scenarios where enterprise customers already have an identity authentication system, federated SSO can be achieved through the IdP.
- **Simplified identity verification login process**
  With the login code provided by the IdP, enterprise customers can complete federated identity verification with Tencent Cloud at a low cost, facilitating a convenient transition to the cloud.

Overview of SAML Role-Based SSO

Last updated：2024-01-26 17:50:17

During role-based SSO with Tencent Cloud, Tencent Cloud acts as the Service Provider (SP), while the enterprise's own identity management system serves as the Identity Provider (IdP). With role-based SSO, enterprises can manage employee information in their local IdP, eliminating the need for user synchronization between Tencent Cloud and the enterprise IdP. Enterprise employees will log in to Tencent Cloud using the specified CAM roles.

Fundamental Procedure

Enterprise employees can access Tencent Cloud via the console or programmatically.

Accessing Tencent Cloud via the Console

Once the administrator has completed the necessary role-based SSO configurations, enterprise employees can log in to Tencent Cloud using the following method. The fundamental procedure is as follows:

1. Utilize a browser to select Tencent Cloud as the target service on the IdP's login page.
2. The IdP generates a SAML response and returns it to the browser.
3. The browser is redirected to the SSO service page and forwards the SAML response to the SSO service.
4. The SSO service uses a SAML response to request temporary security credentials from Tencent Cloud's STS service, and generates a URL that can be used to log in to the Tencent Cloud console with these temporary security credentials.
5. The SSO service returns the URL to the browser.
6. The browser redirects to this URL, logging in to the Tencent Cloud Console with the specified CAM role.

Accessing Tencent Cloud Programmatically

Enterprise employees can access Tencent Cloud by writing a program. The fundamental procedure is as follows:

1. Initiate a login request to the enterprise IdP programmatically.
2. The IdP generates a SAML response containing a SAML assertion about the logged-in user and returns this response to the program.
3. Programmatically invoke the APIAssumeRoleWithSAML provided by Tencent Cloud STS service, passing the following information: the ARN of the IdP in Tencent Cloud, the ARN of the role to be assumed, and the SAML assertion from the enterprise IdP.
4. The STS service will validate the SAML assertion and return a temporary security credential to the program.
5. Programmatically use temporary security credentials to invoke Tencent Cloud APIs.

Configuration steps

To establish a trust relationship between Tencent Cloud and the enterprise IdP, it is necessary to configure SAML for Tencent Cloud as the SP and for the enterprise IdP. Role SSO can only be performed after these configurations are completed.

1. To establish trust between Tencent Cloud and the enterprise IdP, it is necessary to configure the enterprise IdP in Tencent Cloud. For more information, see Create a SAML IdP .
2. Enterprises need to create a CAM role for SSO in the Cloud Access Management Console or programmatically and grant the necessary permissions. For more information, see Creating a CAM Role with an Identity Provider as the Role Carrier .
3. To establish trust from the enterprise IdP to Tencent Cloud, it is necessary to configure Tencent Cloud as a trusted SAML SP within the enterprise IdP and set up the SAML assertion attributes.

Configuration Example

Azure Active Directory Single Sign-On Guide for Tencent Cloud

Overview of OIDC Role Single Sign-On (SSO)

Last updated：2024-01-26 17:52:09

OpenID Connect (OIDC) is an authentication protocol built on the foundation of OAuth 2.0. Tencent Cloud CAM supports OIDC-based SSO of roles.

Concepts

Concept	Note
OIDC	OpenID Connect (OIDC) is an authentication protocol built on the foundation of OAuth 2.0. While OAuth is an authorization protocol, OIDC constructs an identity layer on top of it. In addition to the authorization capabilities provided by OAuth, it also allows clients to verify the identity of end users and obtain their basic information through the API of the OIDC protocol (in the form of HTTP RESTful).
OIDC Token	OIDC can issue identity tokens representing logged-in users to applications, known as OIDC Tokens. OIDC Tokens are utilized to retrieve the basic information of logged-in users.
Temporary ID Credential	Security Token Service (STS) is a temporary access permission management service provided by Tencent Cloud. It allows for the acquisition of temporary identity credentials (STS Token) with customizable validity periods and access permissions.
Issuer URL	The Issuer URL, provided by the external IdP, corresponds to the 'iss' field value of the OIDC Token. The Issuer URL must start with https and conform to the standard URL format. It should not contain query parameters (indicated by ?), fragment sections (indicated by #), or login information (indicated by @).
Client ID	When your application is registered with an external IdP, a Client ID is generated. When you apply for an OIDC token issuance from an external IdP, you must use this client ID. The issued OIDC token will also carry this client ID in the 'aud' field. When creating an OIDC identity provider, this client ID is configured. Then, when using the OIDC token to exchange for an STS Token, Tencent Cloud verifies whether the client ID carried in the 'aud' field of the OIDC token matches the client ID configured in the OIDC identity provider. Role assumption is only permitted when they are consistent.

Scenarios

When enterprise applications need to frequently access Tencent Cloud, using a fixed access key (AccessKey) can pose a security risk if adequate security measures are not in place and the AccessKey is leaked. To address this issue, some enterprises register their applications with their own or third-party identity providers that support OIDC (such as Google G Suite or Okta), to generate OIDC Tokens for the applications using the capabilities of the OIDC identity provider. In this scenario, with the role-based SSO capability provided by Tencent Cloud CAM, enterprise applications can exchange their OIDC Tokens for Tencent Cloud STS Token, thereby securely accessing Tencent Cloud resources.

Moreover, some individual developers or small and medium-sized enterprises allow their employees to log in to Tencent Cloud using their identities registered on certain websites (such as social networking websites). If these websites support the generation of OIDC Tokens, Tencent Cloud CAM can be used to accomplish Single Sign-On based on OIDC.

Fundamental Procedure

1. Register an application in an external IdP to obtain the application's Client ID.
2. In Tencent Cloud CAM, create an OIDC identity provider to establish a trust relationship between Tencent Cloud and an external IdP. For specific operations, please see Create an OIDC Identity Provider.

3. In Tencent Cloud CAM, create an OIDC identity provider's CAM role and authorize it. For specific operations, please see Create an OIDC Identity Provider's CAM Role.
4. Issue an OIDC Token in an external IdP.
5. Utilize the OIDC Token to exchange for an STS Token. For specific operations, please see AssumeRoleWithWebIdentity.
6. Access Tencent Cloud resources using STS Token.

Configuration Example

Azure Active Directory Single Sign-On Guide for Tencent Cloud

SAML 2.0-Based Federation

Last updated：2024-01-26 17:53:34

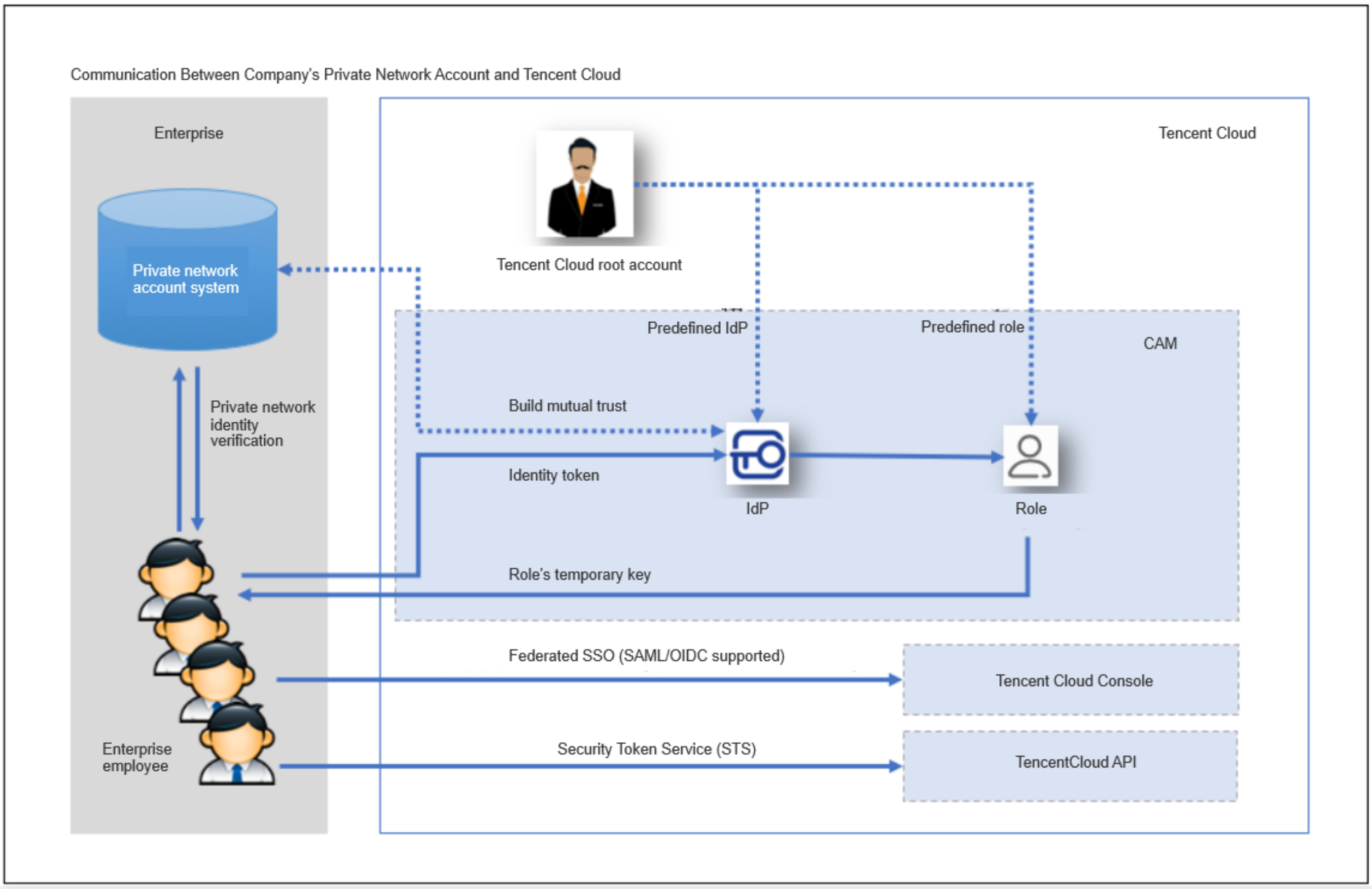
Tencent Cloud supports federated identity authentication based on Security Assertion Markup Language 2.0 (SAML 2.0), an open standard used by many Identity Providers (IdPs). With an IdP, you can implement Federated Single Sign-On (SSO), allowing users authenticated by the federation to log in to the Tencent Cloud Management Console or invoke Tencent Cloud APIs without having to create a CAM sub-user for each member of your enterprise or organization. As SAML 2.0 is a universal open protocol, there is no need to write custom identity proxy code, simplifying the process of federated identity authentication in Tencent Cloud.

SAML IdP

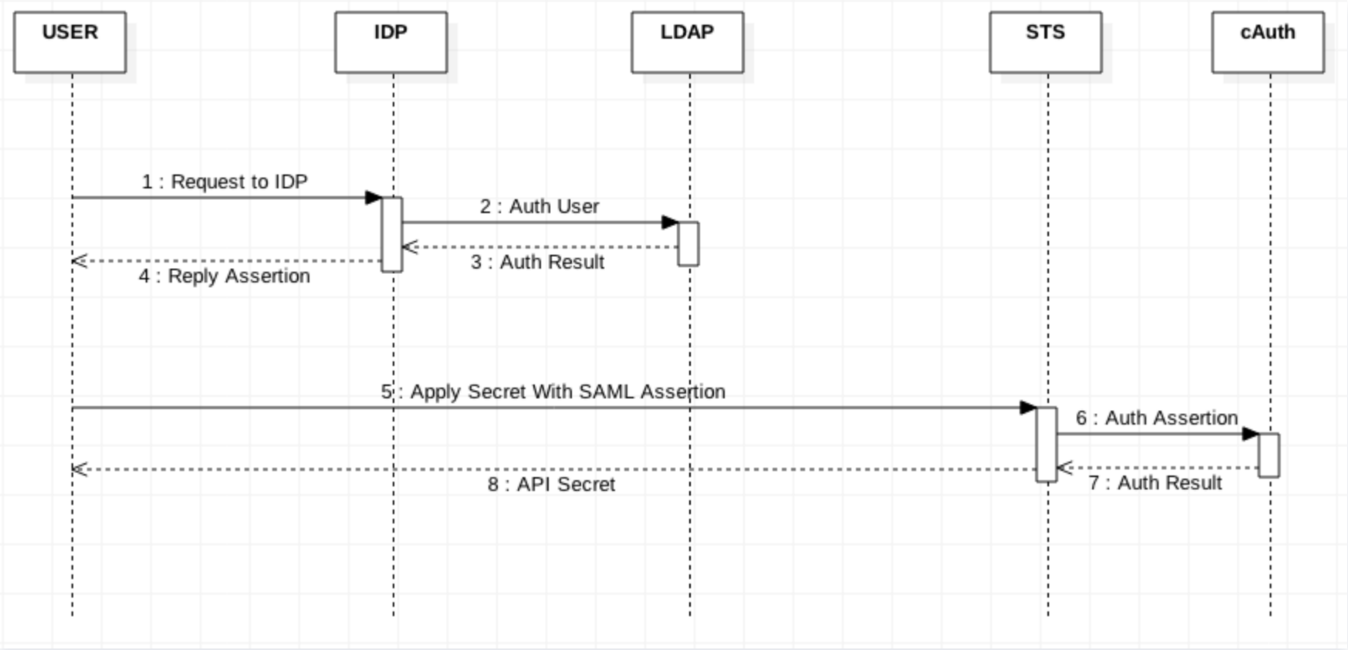
An IdP is an entity in Cloud Access Management (CAM), which can be considered as a collection of external trusted accounts. An IdP for federated identity authentication based on SAML 2.0 describes the services of an IdP that supports the SAML 2.0 (Security Assertion Markup Language 2.0) standard. If you intend to establish trust between a SAML 2.0 protocol-compatible IdP (such as Microsoft Active Directory Federation Services) and Tencent Cloud, so that members within your enterprise or organization can access Tencent Cloud resources, you need to create a SAML IdP. For information on creating a SAML IdP, see Create IdP.

IdP Role

After creating a SAML provider, you must create one or more IdP roles with the SAML Identity Provider as the role entity. A role is a virtual identity with a set of permissions, and temporary security credentials are used when accessing resources. In the context of a SAML 2.0 assertion, the role can be assigned to federated users whose identities have been verified by the Identity Provider (IdP). This role allows the Identity Provider to request temporary security credentials for accessing Tencent Cloud resources. The policy associated with this role determines the access scope of federated users on Tencent Cloud resources. For information on creating roles for Identity Providers based on SAML 2.0 federated identity authentication, please refer to Create Role.

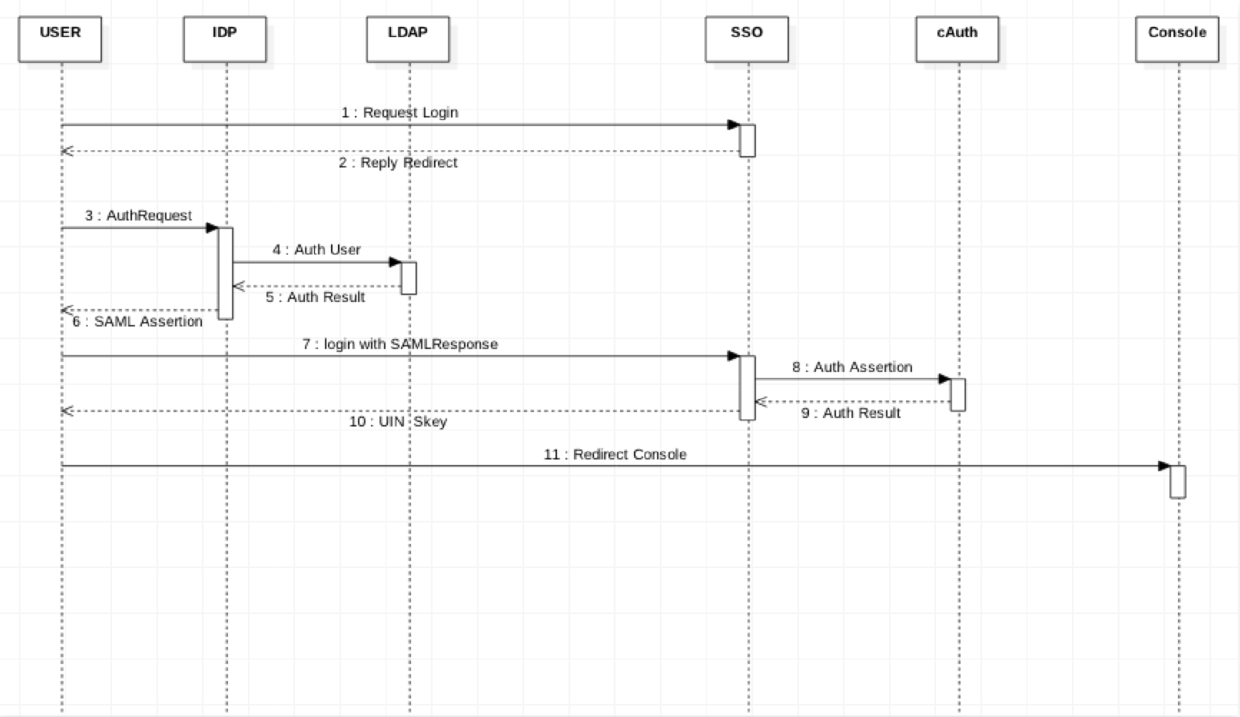

Communication Between Company's Private Network Account and Tencent Cloud
Enterprise
Private network account system
Private network identity verification
Enterprise employee
Tencent Cloud
Tencent Cloud root account
Predefined IdP
Predefined role
CAM
Build mutual trust
Identity token
IdP
Role
Role's temporary key
Federated SSO (SAML/OIDC supported)
Tencent Cloud Console
Security Token Service (STS)
TencentCloud API

Accessing Tencent Cloud APIs via SAML 2.0-Based Federation



1. A user in your enterprise or organization uses a client app to request authentication from your organization's IdP.
2. The IdP authenticates the user against your enterprise's identity authorization system.
3. The user authentication result is returned.
4. The IdP generates a standard SAML 2.0 assertion document based on the user authentication result and sends it back to the client app.
5. The client applies for temporary security keys by sending a sts:AssumeRoleWithSAML request, based on the SAML 2.0 assertion, the resource description of the IdP, and the resource description of the IdP role in use.
6. STS verifies the SAML 2.0 assertion.
7. The verification result is returned.
8. The API applies for a temporary credential based on the result, and sends it to the client.

Realizing Federated Single Sign-on (SSO) via SAML 2.0-Based Federation



1. Enterprise or organization users access Tencent Cloud services via a browser.

2. Tencent Cloud service returns the authentication request to the browser.
3. The browser is redirected to the enterprise organization's IdP.
4. Enterprise verifies user identity.
5. Upon successful authentication of the enterprise user, the user information is returned to the IdP.
6. The IdP generates a standard SAML 2.0 assertion, which is returned to the browser.
7. The browser redirects the SAML 2.0 assertion to Tencent Cloud.
8. Initiate Tencent Cloud SSO login service, request cAuth, and authenticate user identity.
9. Return Tencent Cloud authentication results.
10. Verification succeeded. Returning login status.
11. Redirect to the Tencent Cloud Console service.

Accessing Tencent Cloud Console as SAML 2.0 Federated Users

Last updated：2024-01-26 17:54:37

Scenario

Tencent Cloud supports federated identity authentication based on SAML 2.0 (Security Assertion Markup Language 2.0), an open standard used by many Identity Providers (IdPs). By integrating IdPs with Tencent Cloud through SAML 2.0 federated identity authentication, you can enable automatic login (Single Sign-On) to the Tencent Cloud Console for IdP users to manage Tencent Cloud resources, eliminating the need to create a CAM sub-user for each member of your enterprise or organization.

Instructions

This process creates one or multiple roles for IdPs to log in to the Tencent Cloud console. After being granted permissions, the users can manage the resources of the root account in the console within the scope of permissions.

1. Access the IdP's portal in a browser and select to be redirected to the Tencent Cloud console.
2. The portal can verify the identity of the current user.
3. Upon successful verification, the portal will generate a SAML 2.0 authentication response, which includes assertions identifying the user's identity and related attributes. This response is then sent to the client's browser.
4. The client browser will be redirected to the Tencent Cloud SSO endpoint node and publish an SAML assertion.
5. The endpoint node will request temporary security credentials on behalf of the user and create a console login URL that uses these credentials.
6. Tencent Cloud will return the login URL to the user's client as a redirect.
7. The client browser will be redirected to the Tencent Cloud console. If the SAML 2.0 authentication response includes attributes mapped to multiple CAM roles, the system will first prompt the user to select the role to be used for console access.

From the user's perspective, the entire process is transparent: users start their operations on your organization's internal portal and end them on the Tencent Cloud Console, without needing to provide any Tencent Cloud credentials. For an overview of how to configure this behavior and links to detailed steps, see the following sections.

Configuring SAML 2.0-based IdP in organization

Within your enterprise organization, configure an identity store (such as Azure Active Directory) to use a SAML 2.0-based IdP, such as Azure Active Directory, OneLogin, Okta, etc. By using an IdP, you can generate a metadata document that describes your enterprise organization as an IdP containing authentication keys. This will configure your enterprise organization's portal to route user requests to access the Tencent Cloud Console to Tencent Cloud endpoints for authentication using SAML 2.0 assertions. How you configure your IdP to generate a metadata.xml file depends on your IdP. See your IdP's documentation for instructions, or see the following documents.

- Azure Active Directory Single Sign-On Guide for Tencent Cloud
- OneLogin Single Sign-On Guide for Tencent Cloud
- Okta Single Sign-On Guide for Tencent Cloud
- ADFS Single Sign-On Guide for Tencent Cloud

Creating SAML IdP in CAM

You can create a SAML 2.0 IdP in the Cloud Access Management (CAM) Console. This IdP is an entity in CAM, which can be considered as a collection of trusted external accounts. A SAML 2.0 federated IdP describes an IdP service that supports the SAML 2.0 (Security Assertion Markup Language 2.0) standard. During the creation process, you can upload the metadata document of the IdP in Configure a SAML 2.0 IdP in your organization. For more details, see Create IdP.

Configuring permissions in Tencent Cloud for SAML provider user

You can create a role to establish a trust relationship between your enterprise's IdP and Tencent Cloud. In the context of a SAML 2.0 assertion, this role can be assigned to federated users whose identities have been authenticated by the IdP. This role allows the IdP to request temporary security credentials for accessing Tencent Cloud resources. During this process, you can associate policies with the role and set conditions for its use, thereby determining the scope and conditions of access for federated users to Tencent Cloud resources. For more details, see Create a Role for Your IdP.

Configuring SSO for IdP

Download and save the Tencent Cloud federation metadata XML document at http://cloud.tencent.com/saml.xml. Map the attributes of your organization's IdP to Tencent Cloud's attributes to establish a trust relationship between your organization's IdP and Tencent Cloud. The method of installing this file depends on your IdP. Some providers offer the option to enter this URL, in which case the IdP will retrieve and install the file for you. Other providers require you to download the file from this URL and provide it as a local file. See your IdP's documentation for instructions, or see the following documents.

- Azure Active Directory Single Sign-On Guide for Tencent Cloud
- OneLogin Single Sign-On Guide for Tencent Cloud
- Okta Single Sign-On Guide for Tencent Cloud
- ADFS Single Sign-On Guide for Tencent Cloud

Sample SAML response

Below is an SAML sample:

```
<samlp:Response>
    <saml:Issuer>...</saml:Issuer>
    <ds:Signature>
            ...
    </ds:Signature>
    <samlp:Status>
        ...
    </samlp:Status>
    <saml:Assertion>
        <saml:Issuer>...</saml:Issuer>
        <saml:Subject>
            <saml:NameID>${NameID}</saml:NameID>
            <saml:SubjectConfirmation>
                ...
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions>
            <saml:AudienceRestriction>
                <saml:Audience>${Audience}</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement>
            ...
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="https://cloud.tencent.com/SAML/Attributes/RoleSessionName">
                ...
            </saml:Attribute>
            <saml:Attribute Name="https://cloud.tencent.com/SAML/Attributes/Role">
                ...
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

The `AttributeStatement` element of an SAML assertion must contain the following `Attribute` elements required by Tencent Cloud:

1. The Attribute element with the Name attribute value of https://cloud.tencent.com/SAML/Attributes/Role is mandatory and can be multiple. The AttributeValue element it contains represents the roles that the current user is allowed to assume. The value is a combination of the role description and the IdP description, separated by a comma (,).

> **Note**
> If there are multiple roles, they will be listed for the user to choose from when logging in to the console.
> Below is a sample `Attribute` element of `Role` :

```
<Attribute Name="https://cloud.tencent.com/SAML/Attributes/Role">
  <AttributeValue>qcs::cam::uin/{AccountID}:roleName/{RoleName1},qcs::cam::uin/{AccountID}:saml-
provider/{ProviderName1}</AttributeValue>
  <AttributeValue>qcs::cam::uin/{AccountID}:roleName/{RoleName2},qcs::cam::uin/{AccountID}:saml-
provider/{ProviderName2}</AttributeValue>
</Attribute>
```

If the same IdP is used, you can combine the values into one value and separate the `ARN` of different roles by semicolon (;).

```
<Attribute Name="https://cloud.tencent.com/SAML/Attributes/Role">
<AttributeValue>qcs::cam::uin/{AccountID}:roleName/{RoleName1};qcs::cam::uin/{AccountID}:roleName/{RoleName2},q
cs::cam::uin/{AccountID}:saml-provider/{ProviderName}</AttributeValue>
</Attribute>
```

Note

In the Role source attribute, replace {AccountID}, {RoleName}, and {ProviderName} with the following content:

- Replace {AccountID} with your Tencent Cloud primary account ID, which can be viewed in Account Information - Console.
- Replace {RoleName} with the name of the role you created for the IdP in Tencent Cloud (click to see how to create a role for the IdP in Tencent Cloud here). You can view the role name in the Roles - Console.
- Replace {ProviderName} with the name of the SAML IdP you created in Tencent Cloud. You can view this in the IdP Console.

2. An Attribute element with the Name attribute value of https://cloud.tencent.com/SAML/Attributes/RoleSessionName. This element is mandatory and can only be one. This field is user-defined and should not exceed 32 characters. Below is an example of a RoleSessionName Attribute element. In this example, "userName" can be replaced with your custom information.

```
<Attribute Name="https://cloud.tencent.com/SAML/Attributes/RoleSessionName">
<AttributeValue>userName</AttributeValue>
</Attribute>
```

Creating a SAML IdP

Last updated：2024-01-26 17:55:54

Creating a SAML IdP

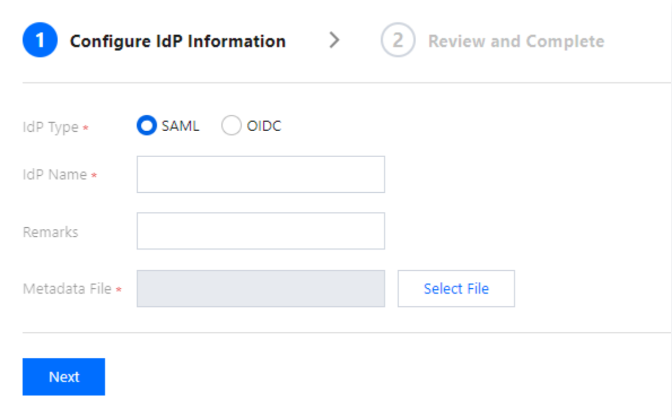
You can create an (identity provider) IdP via either Cloud Access Management Console or CAM API.

Creating a Role via Console

1. To create a SAML IdP, you need to obtain a federation metadata document from your IdP. This document includes the publisher's name and the key to verify the SAML assertions received from the IdP.

> **Note**
> The metadata document is an XML file encoded in UTF-8 format without a Byte Order Mark (BOM). The document size is limited to 40KB. If it exceeds this size, you can manually modify the metadata document, retaining only the elements mentioned above.

2. Log in to the Cloud Access Management Console and navigate to the Identity Providers > Role SSO page, then click on **Create Provider**.
3. On the Create Identity Provider page, select the provider type as SAML, configure the provider information, and click **Next**.
    - IdP Name: Enter the name of the identity provider.
    - Remarks: Enter any notes or comments you have about the current IdP.
    - Metadata File: You need to upload the SAML metadata document that you downloaded in step 1 of the **Upload Metadata Document** process. The upload will be successful once the content of the metadata document is verified as valid.



4. Review the information you have entered about the IdP. Once you have confirmed that everything is correct, click **Complete** to create an IdP.

Creating a role using API

To create an IdP and upload the metadata document, invoke the CreateSAMLProvider interface.

Creating OIDC Identity Provider

Last updated：2024-01-26 17:56:46

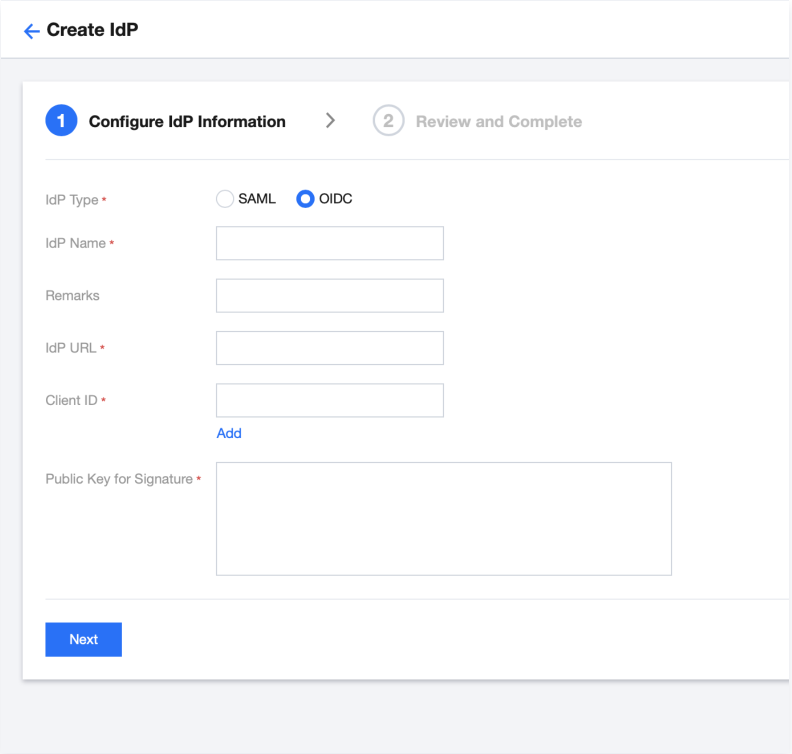
You can create an (identity provider) IdP via either Cloud Access Management Console or CAM API.

Creating a Role via Console

1. To create an OIDC IdP, you need to obtain a federation metadata document from the IdP. This document includes the publisher's name, client ID, IdP URL, and the public key to verify the signature received from the IdP.

> **Note**
> This document uses Azure Active Directory as an example of an IdP.

2. Log in to the Cloud Access Management Console and navigate to the Identity Providers > Role SSO page, then click on **Create Provider**.
3. On the Create Identity Provider page, select the provider type as SAML, configure the provider information, and click **Next**.
   - IdP Name: Enter the name of the identity provider.
   - IdP URL: The identifier for the OpenID Connect identity provider. This corresponds to the "issuer" field value in the OpenID Connect metadata document provided by the identity provider.
   - Client ID: The client ID registered with the OpenID Connect IdP. This can be obtained from the **Azure Active Directory > Enterprise Applications > OIDCSSO Application Overview page**.
   - Public Key for Signature: This is the public key used to verify the signature of the IdP's ID Token. It corresponds to the content linked in the "jwks_uri" field in the OpenID Connect metadata document provided by the IdP (open the link in a browser to obtain the content). For the security of your account, it is recommended that you rotate the signature public key regularly.



4. Click 'Next' to review the information you've entered about the identity provider. Once you've confirmed that everything is correct, click on **Complete** to create the identity provider.

Creating a role using API

To create an IdP and upload the metadata document, please invoke the CreateOIDCConfig interface.

Managing IdPs

Last updated：2024-01-26 17:58:35

Deleting SAML IdPs

You can manage your IdPs using the Cloud Access Management Console or CAM API.

Delete via the Console

1. Log in to the Cloud Access Management (CAM) console and navigate to the Identity Providers > Role-Based SSO page.
2. In the list of IdPs for your account, select the IdP you want to delete and click **Delete** in the **Operation** column.
3. When deleting an IdP, you will be requested to confirm the deletion. Click **OK** to delete the IdP.

Delete via API

- (Optional) To list all IdP information on separate pages, invoke ListSAMLProviders.
- (Optional) To get detailed information about a specific provider, invoke GetSAMLProvider.
- To delete a SAML IdP, invoke the DeleteSAMLProvider operation.

Modifying SAML IdPs

You can modify an IdP using the Cloud Access Management Console or CAM API.

Modifying in the Console

1. Log in to the Cloud Access Management (CAM) console and navigate to the Identity Providers > Role-Based SSO page.
2. In the list of IdPs for your account, select the IdP you intend to modify and click on the provider name to enter the details page.
3. You can upload a metadata file to redefine the current IdP, or download the current metadata file.

Modifying using API

To update the SAML IdP description or metadata document, please invoke UpdateSAMLProvider.

Azure Active Directory Single Sign-On

Last updated：2024-02-01 21:41:58

Scenario

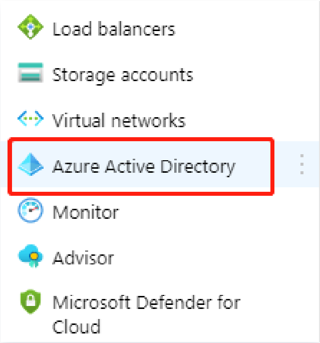
Azure Active Directory (Azure AD) is a cloud-based identity and Cloud Access Management service launched by Microsoft, which aids employees in managing internal and external resources. Tencent Cloud supports federated identity authentication based on SAML 2.0 (Security Assertion Markup Language 2.0), an open standard used by many Identity Providers (IdPs). By integrating Azure Active Directory with Tencent Cloud through SAML 2.0 federated identity authentication, you can enable automatic sign-in (Single Sign-On) to the Tencent Cloud console with Azure AD accounts to manage Tencent Cloud resources, without requiring the creation of a CAM sub-user for each member of the enterprise or organization.

Instructions

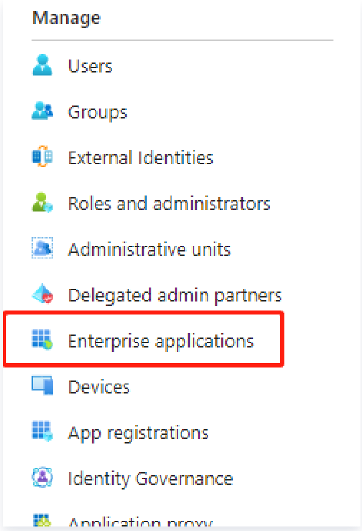
Creating Azure AD Enterprise Applications

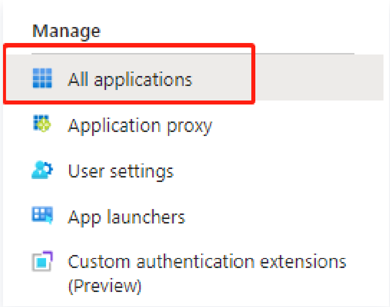
> **Note**
> You can create an Azure AD enterprise application through this step. If you are using one, you can skip this step and go straight to Configure CAM.

1. Navigate to the Azure AD Portal and click on **Azure Active Directory** in the left navigation bar, as shown below:

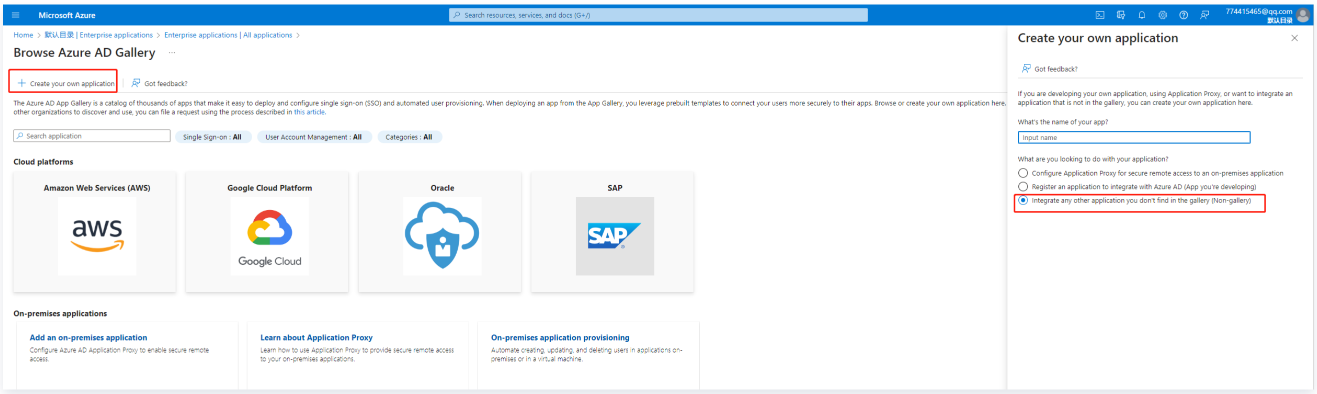


2. Click on **Enterprise applications** and select **All applications** as shown in the image below:





3. Click **Create your own application** to open the "Create your own application" window, and select **Integrate any other application you don't find in the gallery (Non-gallery)**. As shown in the image below:


Microsoft Azure
Search resources, services, and docs (G+/)
774415465@qq.com
默认目录
Home > 默认目录 | Enterprise applications > Enterprise applications | All applications >
Browse Azure AD Gallery
+ Create your own application
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
aws
Google Cloud Platform
Google Cloud
Oracle
SAP
On-premises applications

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. other organizations to discover and use, you can file a request using the process described in this article.

Add an on-premises application
Configure Azure AD Application Proxy to enable secure remote access.

Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

On-premises application provisioning
Automate creating, updating, and deleting users in applications on-premises or in a virtual machine.

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

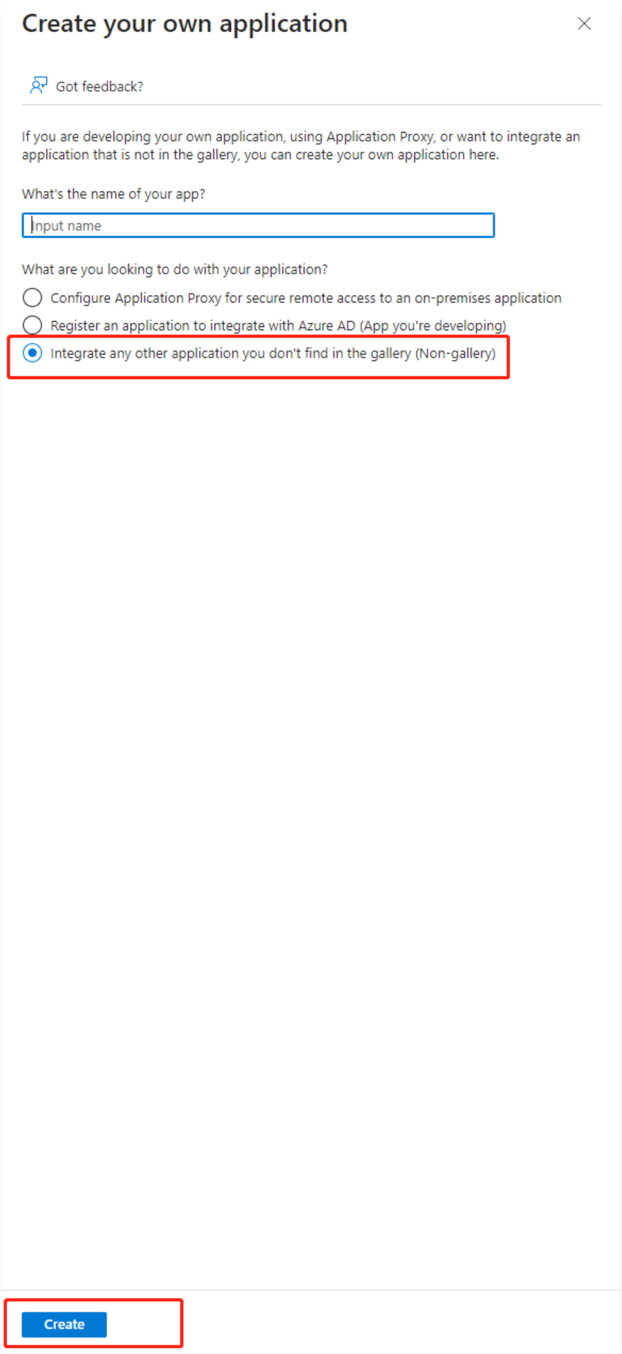
What's the name of your app?

Input name

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application to integrate with Azure AD (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

4. Enter the **Name** and click **Create** to complete the creation of the Azure AD application, as shown in the figure below:



Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Input name

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Azure AD (App you're developing)

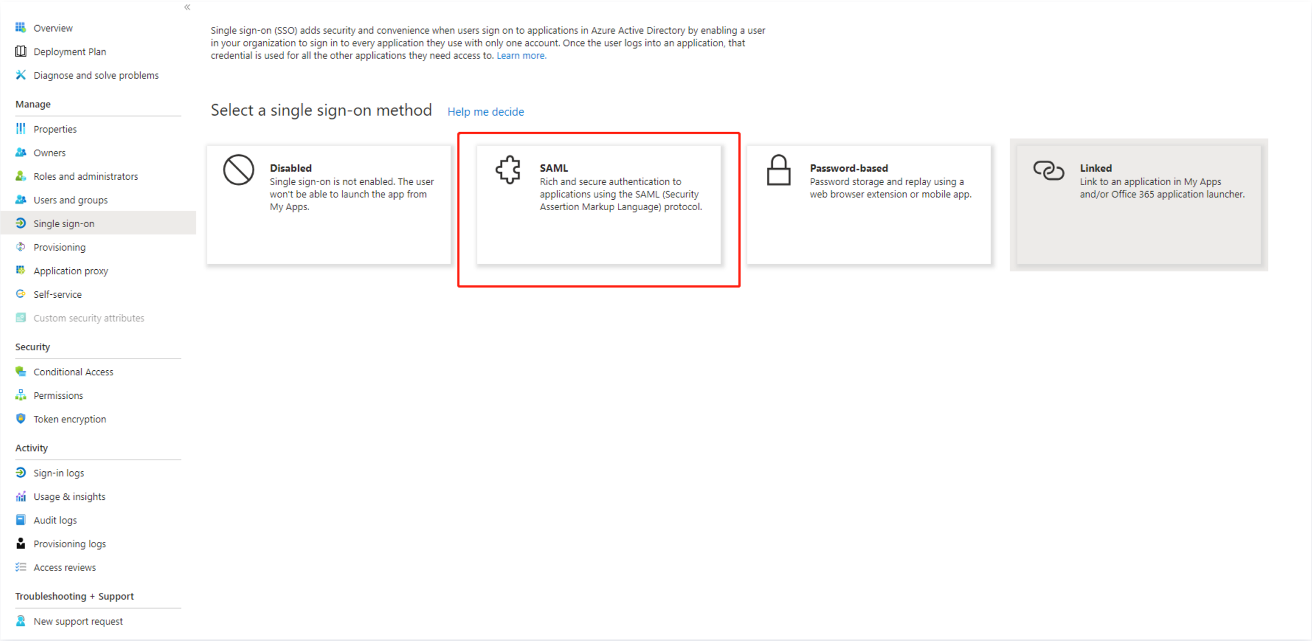
● Integrate any other application you don't find in the gallery (Non-gallery)

Create

Configuring CAM

> **Note**
> This step configures the trust relationship between Azure AD and Tencent Cloud to make them trust each other.

1. In the left sidebar, select **Azure Active Directory** > **Enterprise Applications** > the application you created, to go to the application overview page.
2. Click **Single Sign-On** to open the "Select a single sign-on method" page.
3. In the opened "Select a single sign-on method" page, select **SAML**, as shown below:



Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method Help me decide

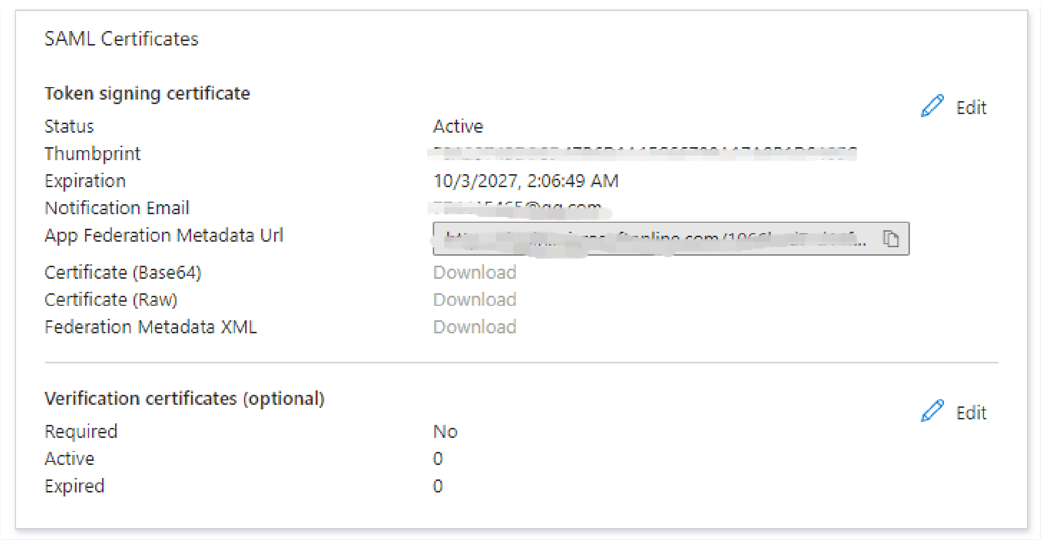
Disabled Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based Password storage and replay using a web browser extension or mobile app.

Linked Link to an application in My Apps and/or Office 365 application launcher.

4. On the preview page of "SAML Single Sign-On", download the **Federation Metadata XML** file from the **SAML Certificate**. As shown below:



SAML Certificates

Token signing certificate Edit

Status	Active
Thumbprint	[redacted]
Expiration	10/3/2027, 2:06:49 AM
Notification Email	[redacted]
App Federation Metadata Url	[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) Edit

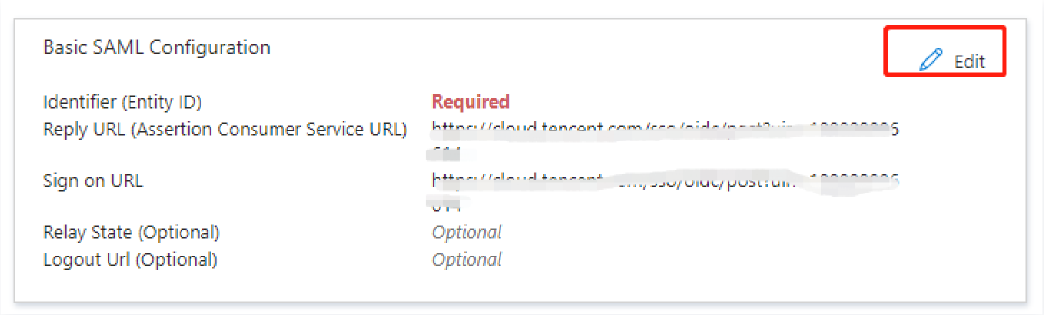
Required	No
Active	0
Expired	0

5. Create a SAML IdP and role in Tencent Cloud. For detailed operations, see Create IdP and Create Role to create a role for the IdP.

Configuring the Azure AD Single Sign-On

Note
This step maps Azure AD application attributes to Tencent Cloud attributes to create trust between the Azure AD application and Tencent Cloud.

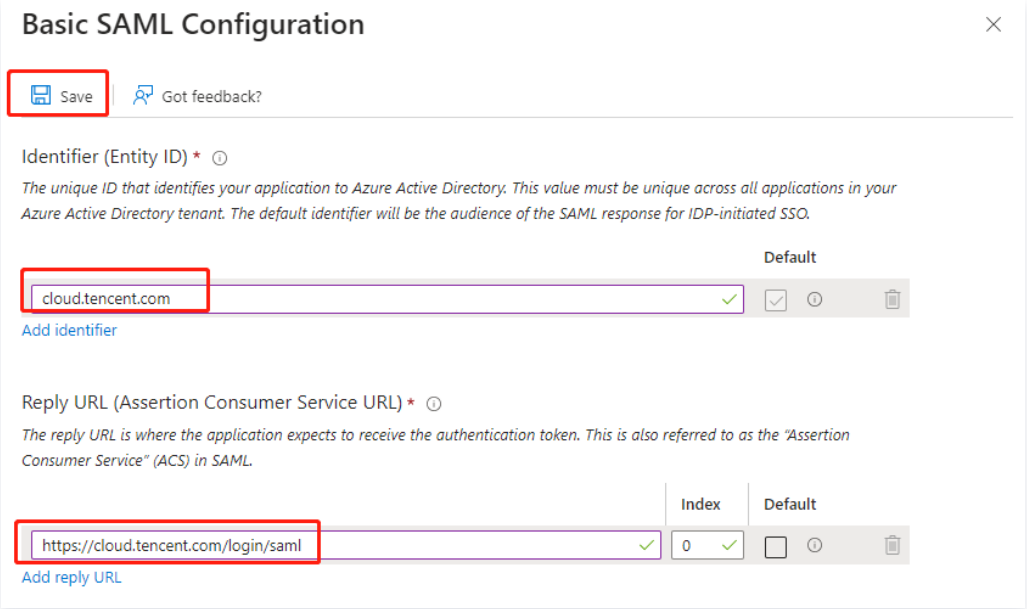
1. In the "SAML Single Sign-On" overview interface, click on the ✎ at the top right corner of "Basic SAML Configuration". As shown below:



Basic SAML Configuration

Identifier (Entity ID) **Required**
Reply URL (Assertion Consumer Service URL) [redacted]
Sign on URL [redacted]
Relay State (Optional) *Optional*
Logout Url (Optional) *Optional*

2. On the "Basic SAML Configuration" edit page, fill in the following information and click **Save**. As shown below:



Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
cloud.tencent.com	☑

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

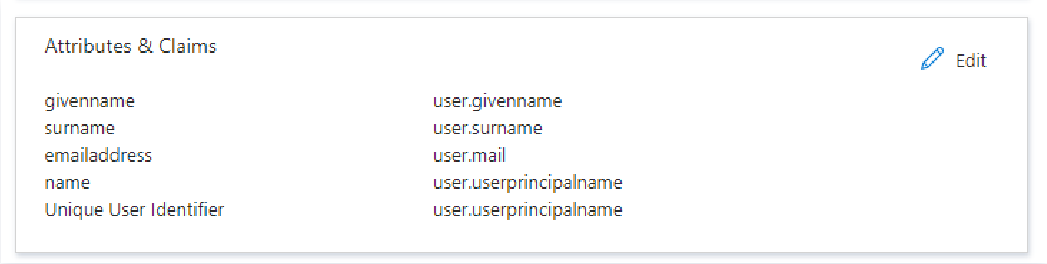
	Index	Default
https://cloud.tencent.com/login/saml	0	□

You can configure based on the site where your Tencent Cloud account is located.

Site	Identifier (Entity ID)	Reply URL (Assertion Consumer Service (ACS) URL)
China website	cloud.tencent.com	https://cloud.tencent.com/login/saml
International website	intl.cloud.tencent.com	https://intl.cloud.tencent.com/login/saml

> **Note**
> The Reply URL (Assertion Consumer Service URL) is the Tencent Cloud page to which you are redirected. If you need to specify another page, you can use the format https://cloud.tencent.com/login/saml?s_url=xxxx, where xxxx is the address you need to specify, which requires urlencode.

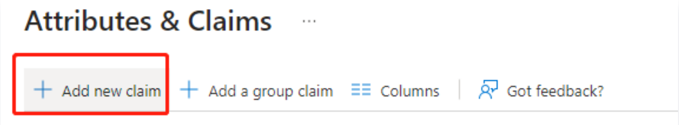
3. In the "SAML Single Sign-On" overview interface, click on the ✎ at the top right corner of "Attributes & Claims" to open the "User Attribute Claims" editing page, as shown below:



Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

4. On the "Attributes & Claims" edit page, click **Add new claim** to navigate to the "Manage Claims" page, as shown below:



5. On the "Manage User Claims" page, add the following two claims and click **Save**.

Name	Namespace	Source	Source Attribute
Role	https://cloud.tencent.com/SAML/Attributes	Properties	qcs::cam::uin/{AccountID}:roleName/{RoleName},qcs::cam::uin/{AccountID}:saml-provider/{ProviderName}
RoleSessionName	https://cloud.tencent.com/SAML/Attributes	Properties	Azure

> **Note**
> Replace `{AccountID}`, `{RoleName}`, and `{ProviderName}` in the source `Role` attribute with the following:
> - Replace {AccountID} with your Tencent Cloud account ID. You can view this at Account Information - Console.
> - Replace {RoleName} with the role name you created in Tencent Cloud for the Identity Provider (click to see how to create a role in Tencent Cloud for the Identity Provider), the role name can be viewed in Roles - Console. If you need to add more, you can add them in this format: qcs::cam::uin/{AccountID}:roleName/{RoleName}, separated by a semicolon (;).
> - Replace {ProviderName} with the name of the SAML identity provider you created in Tencent Cloud. You can view this at Identity Provider - Console.

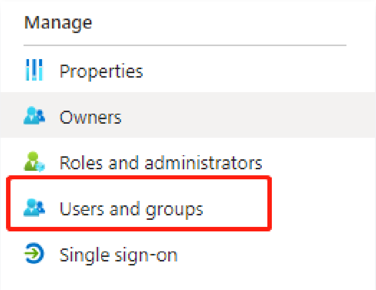
Configuring Azure AD Users

> **Note**
> This step assigns Tencent Cloud SSO access permissions to Azure AD users.

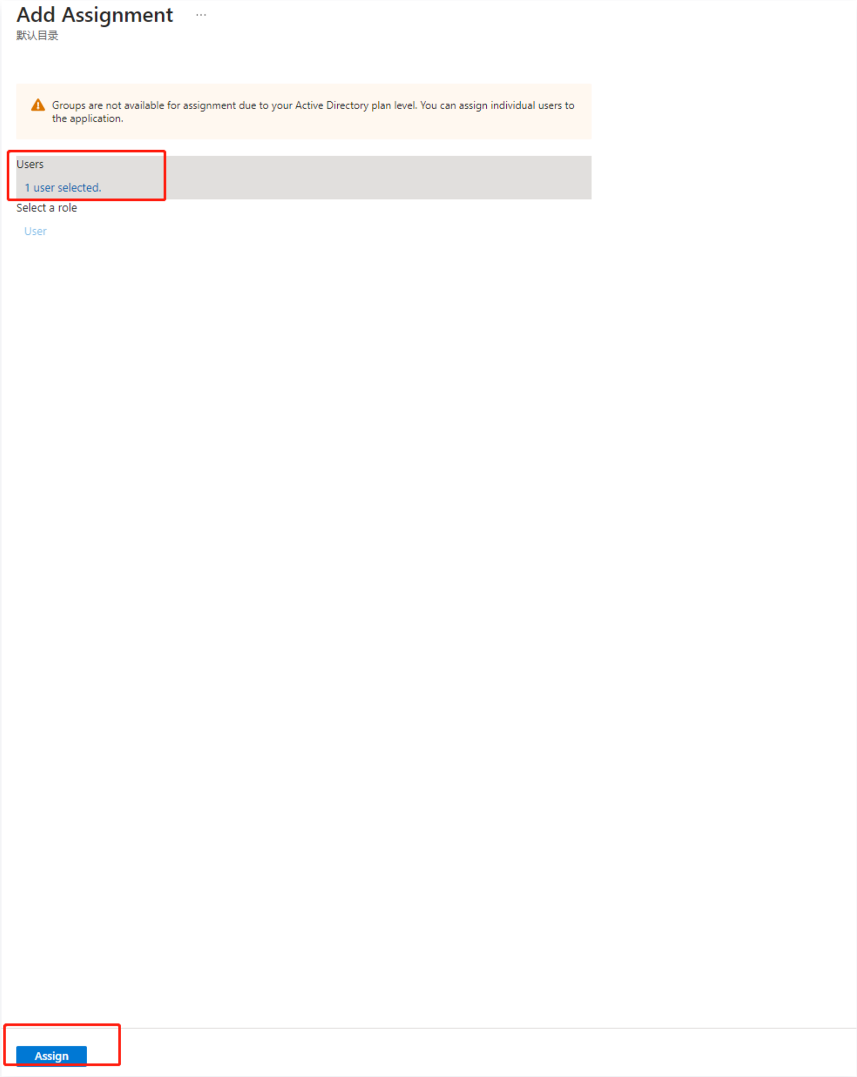
1. Click **Azure Active Directory** in the left sidebar, then click **Users > All Users.**
2. Click on the top left corner**+New User > Create User,** fill in the **Name, Username**, on the "User" page, check **Show Password,** and click **Create** at the bottom to complete the creation once the information is verified.

> **Note**
> The username format is: username@domain. You can customize the username, and the domain can be viewed by clicking **Azure Active Directory** in the left sidebar to open the overview page, where you can see the **initial domain** you set earlier. You can copy and save the username and password for future use.

3. In the left sidebar, select **Azure Active Directory** > **Enterprise Applications** > the application you created to go to the application overview page, and click **Users and groups**. As shown in the figure below:



4. Click **Add User/Group**, select the user you created in Step 2, and click **Select**.
5. Go to the "Add Assignment" page and click **Assign** after confirming as shown below:



Add Assignment

默认目录

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

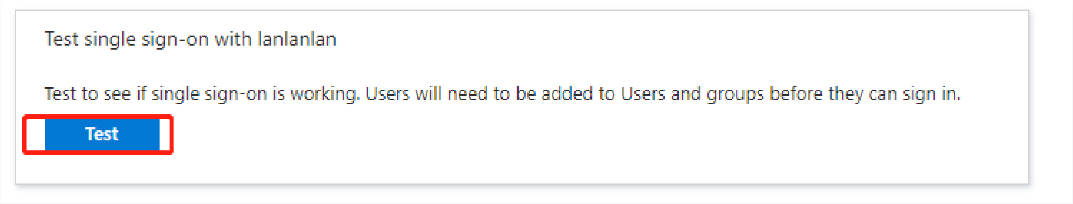
Users

1 user selected.

Select a role

User

6. In the left sidebar, select **Azure Active Directory** > **Enterprise Applications** > the application you created, to go to the application overview page.
7. Click on **Single Sign-On** to open the "SAML Single Sign-On" overview interface, then click **Test**. As shown in the image below:



Test single sign-on with lanlanlan

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

8. On the "Test Single Sign-On" page, select **Log in as Another User**.
9. Enter the username and password you saved in Step 2 to log in to the Tencent Cloud Console.

OneLogin Single Sign-On

Last updated：2024-01-31 17:32:04

Scenario

OneLogin is a provider of cloud identity access management solutions, enabling one-click login to all necessary internal enterprise systems through its identity authentication system. Tencent Cloud supports federated identity authentication based on SAML 2.0 (Security Assertion Markup Language 2.0), an open standard used by many IdPs (IdPs) including OneLogin.

Utilizing an IdP facilitates Federated Single Sign-On (SSO), allowing administrators to authorize users authenticated through federated identity to log in to the Tencent Cloud Management Console or invoke Tencent Cloud APIs. This eliminates the need to create a CAM sub-user for each member within an enterprise or organization.

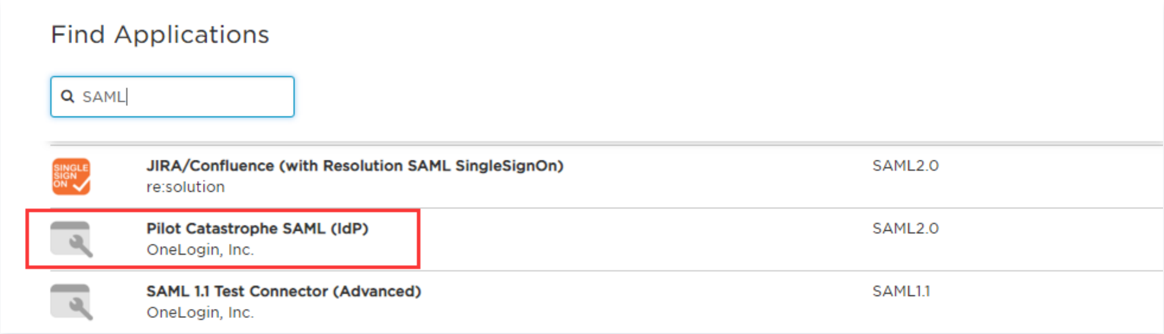
This document describes how to configure OneLogin SSO to Tencent Cloud.

Instructions

Creating a OneLogin enterprise application

> **Note**
> - You can create a OneLogin enterprise application through this step. If you already have an application in use, please ignore this step and proceed to Configure CAM .
> - This document uses the application name **test** as an example.

1. Log in and access the OneLogin website , click on **Applications** to navigate to the application management page.
2. On the Application Management page, click on **ADD APP** in the upper right corner.
3. Enter "SAML" in the search box, press "Enter", and click on **Pilot Catastrophe SAML (IdP)*** in the results list as shown below:

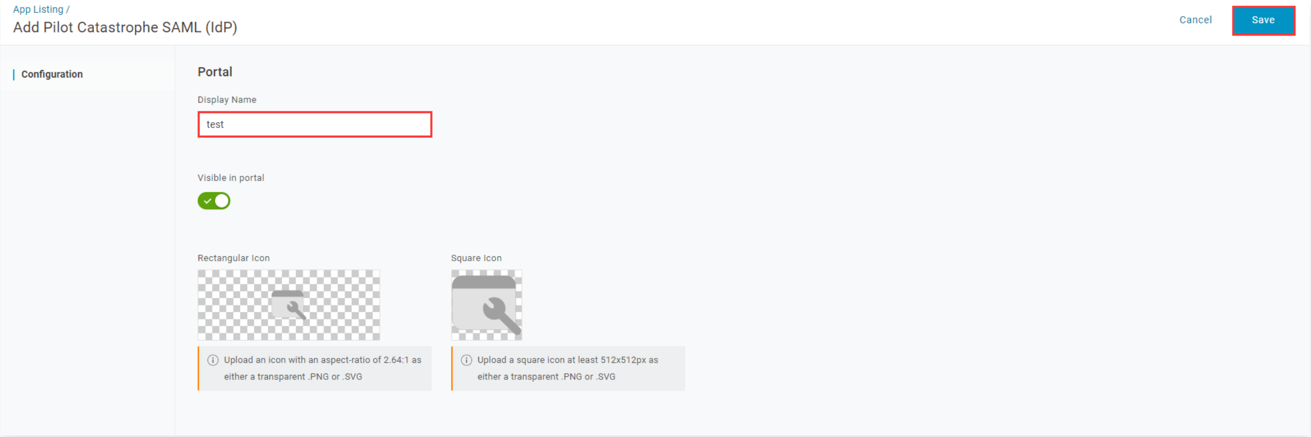


Find Applications

SAML

JIRA/Confluence (with Resolution SAML SingleSignOn) re:solution	SAML2.0
Pilot Catastrophe SAML (IdP) OneLogin, Inc.	SAML2.0
SAML 1.1 Test Connector (Advanced) OneLogin, Inc.	SAML1.1

4. Enter the application name in "Display Name" and click **SAVE** in the upper right corner to complete the creation of the application, as shown below:



App Listing /

Add Pilot Catastrophe SAML (IdP)

Portal

Display Name: test

Visible in portal: on

Rectangular Icon

Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Square Icon

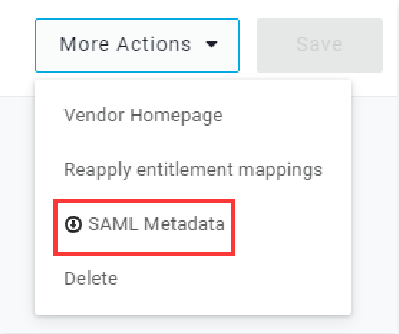
Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

Configuring CAM

> **Note**

- This step configures the trust relationship between OneLogin and Tencent Cloud.
- In this example, the SAML IdP and role name are both **test**.

1. On the OneLogin Application Management page , select the application **test** you have already created.
2. Click on **More Actions** at the top right corner, select **SAML Metadata**, and download the IDP cloud data document. As shown below:

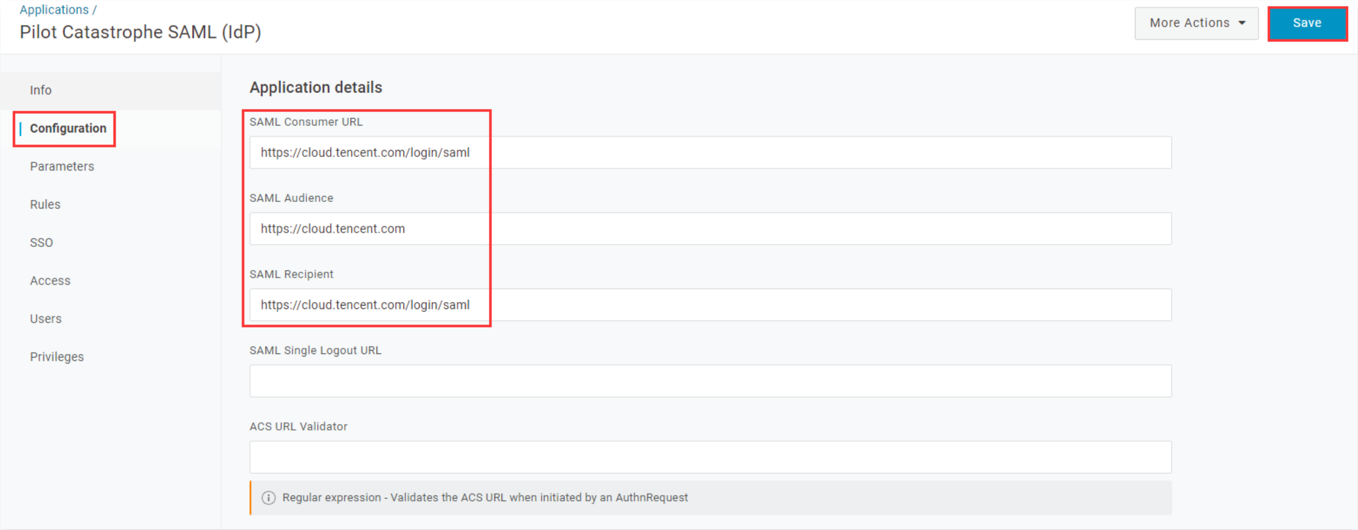


3. Create a Tencent Cloud CAM IdP and role. For detailed operations, see Create IdP and Create Role to create a role for the IdP.

Configuring OneLogin SSO

> **Note**
> This step maps OneLogin application attributes to Tencent Cloud attributes to create the trust between the OneLogin application and Tencent Cloud.

1. On the OneLogin Application Management page , click on the previously created "test" application to navigate to the application editing page.
2. Select the **Configuration** tab, enter the following information, and click **SAVE**, as shown below:



SAML Consumer URL: https://cloud.tencent.com/login/saml
SAML Audience: https://cloud.tencent.com
SAML Recipient: https://cloud.tencent.com/login/saml
SAML Single Logout URL
ACS URL Validator
Regular expression - Validates the ACS URL when initiated by an AuthnRequest

You can configure it based on the site of your Tencent Cloud account:

Site	SAML Consumer URL	SAML Audience	SAML Recipient
China website	https://cloud.tencent.com/login/saml	https://cloud.tencent.com	https://cloud.tencent.com/login/saml
International website	https://intl.cloud.tencent.com/login/saml	https://intl.cloud.tencent.com/login/saml	https://intl.cloud.tencent.com/login/saml

> **Note**

The SAML Recipient is the Tencent Cloud page to which you will be redirected. If you need to specify another page, you can use the format https://cloud.tencent.com/login/saml?s_url=xxxx, where xxxx is the address you need to specify, which requires URL encoding.

3. Click on **Parameters**, and then click + to add the following two configuration details.

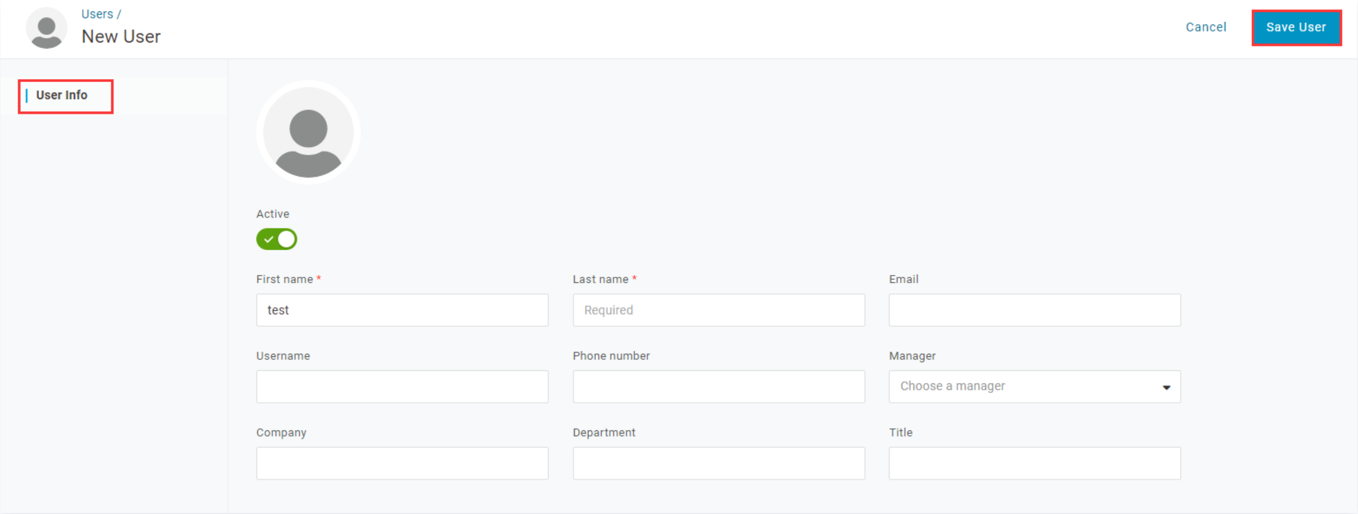
Field name	Flags	Value	Source Attribute
https://cloud.tencent.com/SAML/Attributes/Role	Include in SAML assertion	Macro	qcs::cam::uin/{AccountID}:roleName/{RoleName1};qcs::cam::uin/{AccountID}:roleName/{RoleName2},qcs::cam::uin/{AccountID}:saml-provider/{ProviderName}
https://cloud.tencent.com/SAML/Attributes/RoleSessionName	Include in SAML assertion	Macro	Test

> **Note:**
> - Replace `{AccountID}` , `{RoleName}` , and `{ProviderName}` in the source `Role` attribute with the following:
> - Replace {AccountID} with your Tencent Cloud account ID, which can be viewed in the Account Information - Console .
> - Replace {RoleName} with the name of the role you created in Tencent Cloud. You can view it in the Role - Console .
> - Replace {ProviderName} with the name of the SAML IdP you created in Tencent Cloud. You can check this in the Identity Provider Console .

4. Click **Save** in the upper right corner to save the configuration.

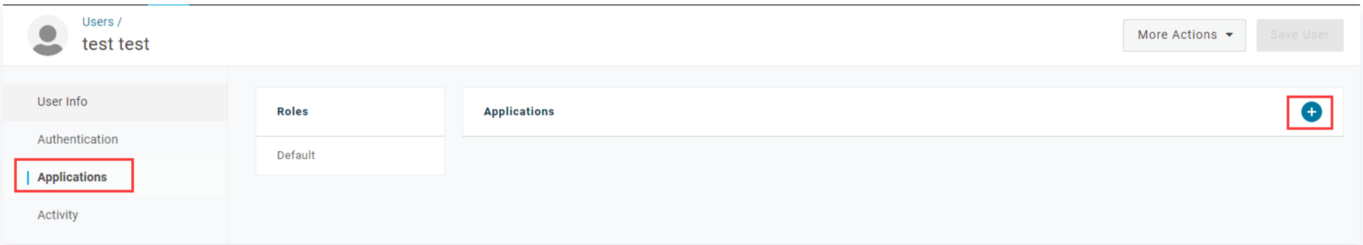
Configuring a OneLogin user

1. Log in and access the OneLogin website , click on **Users** to navigate to the user management page.
2. Click on **New User** in the upper right corner to navigate to the new user page.
3. Enter the "First name", "Last name", "Email", and "Username", then click **Save User** to save. As shown in the figure below:

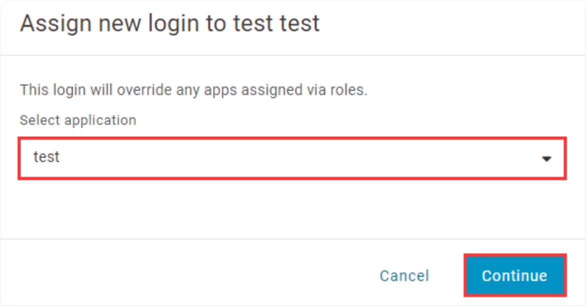


> **Note**
> The account password can be viewed via email, or you can click **MORE ACTIONS** and select **Change Password** to modify the password.

4. Click on **Applications** in the user edit page, and select + on the right, as shown below:



5. In the pop-up dialog box, select the SAML application "test" that you have created, and click **CONTINUE**, as shown below:

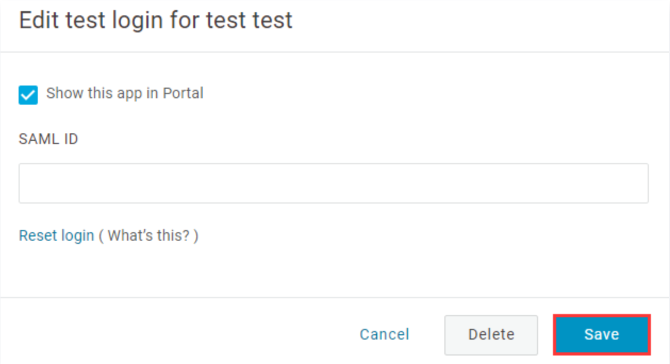

Assign new login to test test

This login will override any apps assigned via roles.

Select application

test

6. On the Edit test login for test test page, click **Save** as shown below:


Edit test login for test test

☑ Show this app in Portal

SAML ID

Reset login (What's this?)

7. Log in to OneLogin using the account created in Step 3 and access the SAML application "test" that was created. This will redirect you to the Tencent Cloud console.

Okta Single Sign-On

Last updated: 2024-01-31 17:34:41

Scenario

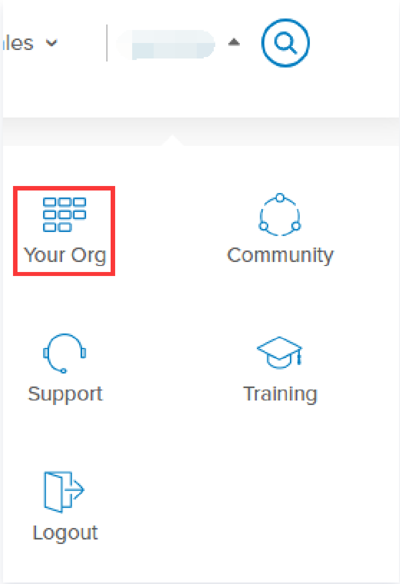
Okta is a provider of identity recognition and access management solutions. Tencent Cloud supports federated identity authentication based on SAML 2.0 (Security Assertion Markup Language 2.0), an open standard used by many Identity Providers (IdPs). By integrating Okta with Tencent Cloud through SAML 2.0 federated identity authentication, you can enable automatic login (Single Sign-On) to the Tencent Cloud console with Okta accounts to manage Tencent Cloud resources, eliminating the need to create a CAM sub-user for each member of your enterprise or organization.

Instructions

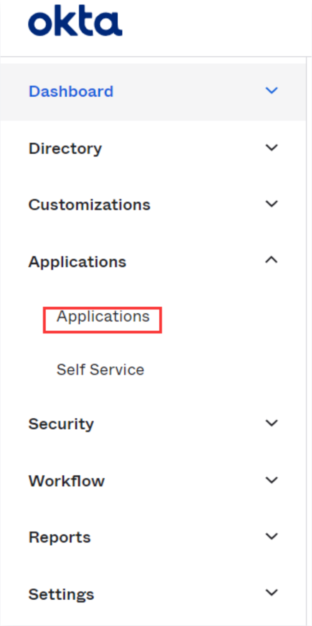
Creating Okta Applications

> **Note**
> You can create an Okta application through this step. If you already have an application in use, you can ignore this operation and proceed to Configure CAM .

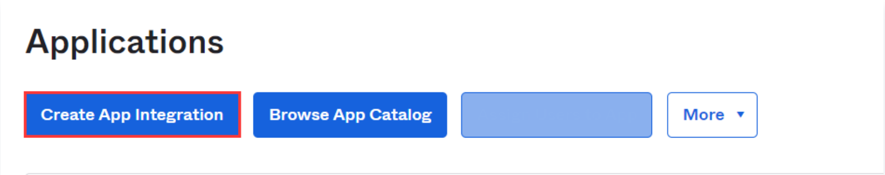
1. Log in to the Okta website , and click on the top right corner **User Name** > **Your Org**, as shown below:



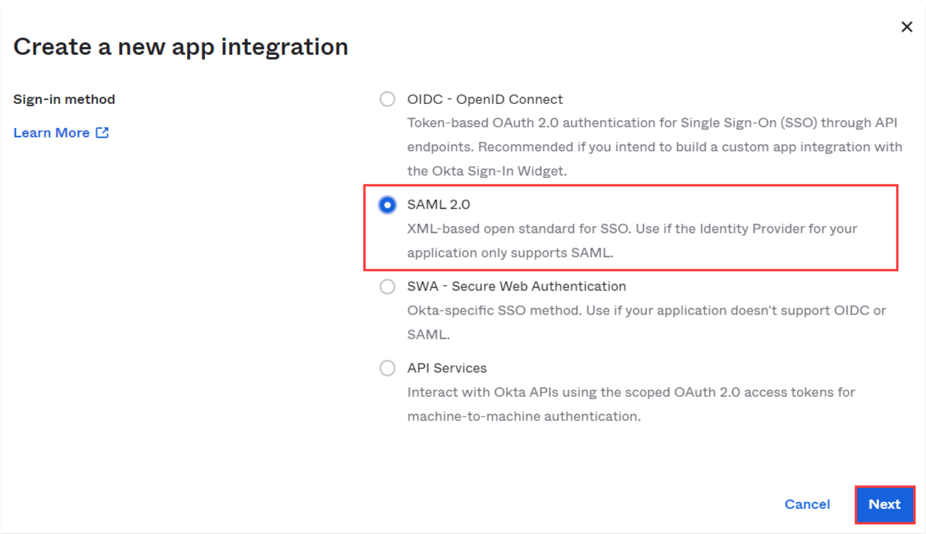
2. On the Okta homepage, click **Admin** in the top-right corner to enter the admin interface.
3. On the administrator page, select Applications to enter the application management page, as shown below:



4. On the Application Management page, click **Add Application** to navigate to the Add Application page.
5. On the Add Application page, click **Create APP Integration** as shown below:



6. In the pop-up window for creating a new application integration, select the Platform and Sign on method, where the Sign on method should be set to SAML 2.0. Click **Create** as shown below:



Create a new app integration

Sign-in method

Learn More

○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

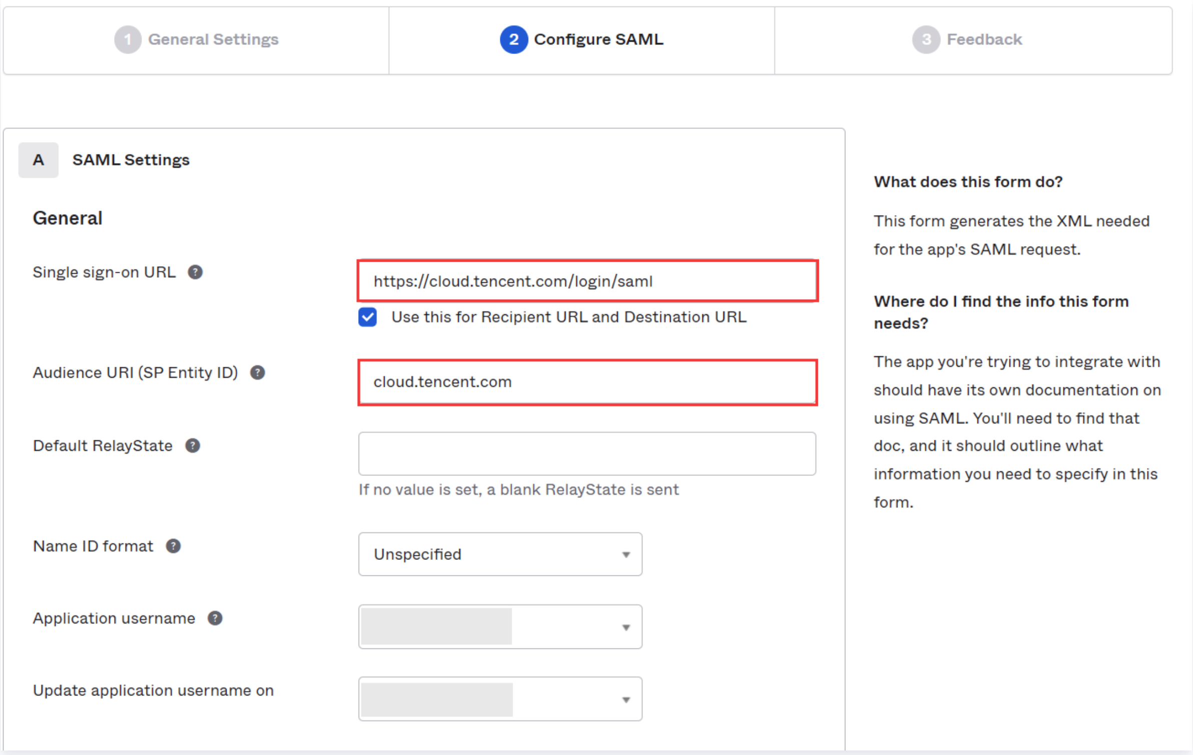
7. On the General Settings page, supplement the App name, App logo (optional), and App visibility (optional) information. Click **Next**. This application can be used to integrate with Tencent Cloud, enabling automatic login (Single Sign-On) to the Tencent Cloud console with Okta accounts to manage Tencent Cloud resources.

Configuring SAML for Okta Applications

Note

- This step maps Okta application attributes to Tencent Cloud attributes to create trust between Okta and Tencent Cloud.
- If you have created an application following the Create Okta Application guide, you can proceed directly to Step 3.

1. Navigate to the Application Management page and click on the name of the application you created.
2. On the General page, click **Edit** under the SAML Settings section, confirm the current App name, App logo (optional), and App visibility (optional) information, and then click **Next** to proceed to the Configure SAML page.
3. On the Configure SAML/Configure SAML page, supplement the Single sign on URL and Audience URL (SP Entity ID) under GENERAL with the following information, as shown in the figure below:



Single sign-on URL: https://cloud.tencent.com/login/saml

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): cloud.tencent.com

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username:

Update application username on:

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

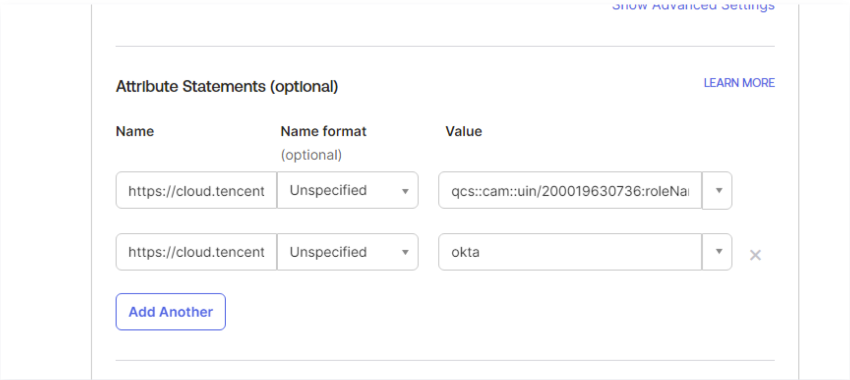
4.

You can configure according to the site where your Tencent Cloud account is located:

Site	Single sign on URL	Audience URL(SP Entity ID)
China website	https://cloud.tencent.com/login/saml	cloud.tencent.com
International website	https://intl.cloud.tencent.com/login/saml	intl.cloud.tencent.com

> **Note**
> The Single Sign-On URL is the Tencent Cloud page to which you will be redirected. If you need to specify a different page, you can use the format `https://cloud.tencent.com/login/saml?s_url=xxxx` , where xxxx is the address you need to specify, which requires urlencode.

5. On the SAML/Configure SAML page, supplement the ATTRIBUTE STATEMENTS under GENERAL with the following information, as shown below:



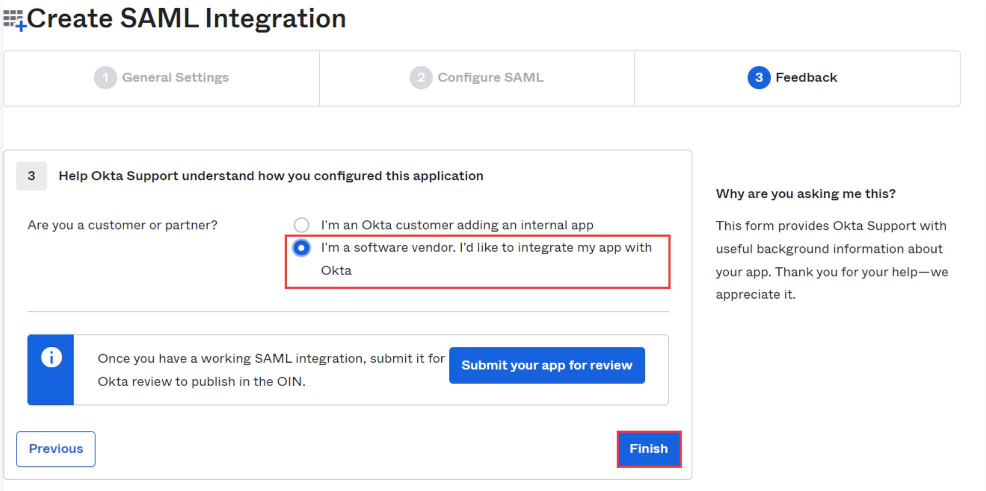
Attribute Statements (optional)

Name	Name format (optional)	Value
https://cloud.tencent	Unspecified	qcs::cam::uin/200019630736:roleNa
https://cloud.tencent	Unspecified	okta

Name	Name format	Value
https://cloud.tencent.com/SAML/Attributes/Role	Unspecified	qcs::cam::uin/{AccountID}:roleName/{RoleName},qcs::cam::uin/{AccountID}:saml-provider/{ProviderName}
https://cloud.tencent.com/SAML/Attributes/RoleSessionName	Unspecified	okta

> **Note**
>
> In Value, replace {AccountID}, {RoleName}, and {ProviderName} with the following content:
> - Replace {AccountID} with your Tencent Cloud account ID. You can view this at Account Information - Console.
> - Replace {RoleName} with the name of the role you created for the IdP in Tencent Cloud (click to see how to create a role for the IdP in Tencent Cloud here). You can view the role name in Roles - Console. If you need to add more, you can follow this format: qcs::cam::uin/{AccountID}:roleName/{RoleName}, separated by a semicolon (;).
> - Replace {ProviderName} with the name of the SAML identity provider you created in Tencent Cloud. You can view this at Identity Provider - Console.

6. Click **Next** to proceed to the Feedback page. After selecting the following information, click **Finish** to complete the CAM operation configuration, as shown below:



Create SAML Integration

3 Help Okta Support understand how you configured this application

Are you a customer or partner?
○ I'm an Okta customer adding an internal app
● I'm a software vendor. I'd like to integrate my app with Okta

Once you have a working SAML integration, submit it for Okta review to publish in the OIN.

Why are you asking me this?

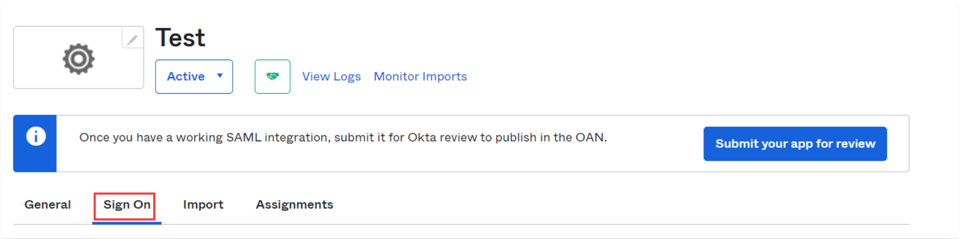
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

Configuring SAML Integration for Okta Applications

> **Note**
> This step configures the trust relationship between Okta and Tencent Cloud.

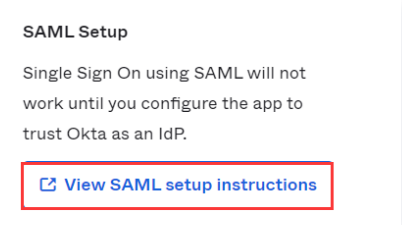
1. Log in to the Admin Interface, select Applications to navigate to the application management page.
2. On the Application Management page, click the name of the application you created to enter the Application Details page, and

then click **Sign On**, as shown below:



Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

3. On the Sign On page, click **View SAML setup instructions** at the bottom right to view the IdP metadata, as shown below:



SAML Setup

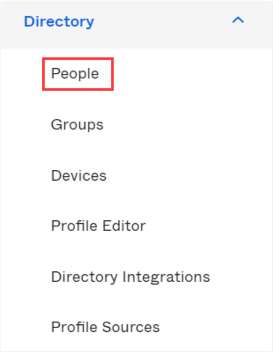
Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

4. After obtaining the identity provider metadata, you can right click on the viewing page to save it locally.
5. Create a SAML IdP and role in Tencent Cloud. For detailed operations, see Create IdP .

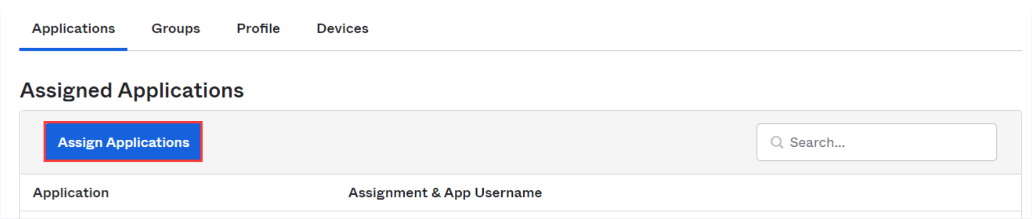
Configuring Okta Users

> **Note**
> This step assigns Tencent Cloud SSO access permissions to Okta users.

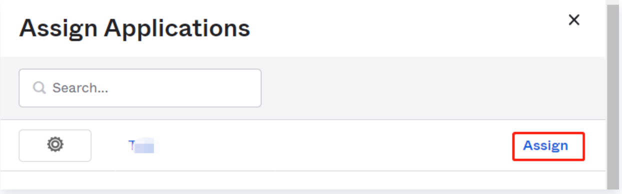
1. Log in to the Admin Interface , click on **People** under Directory to enter the user management page, as shown below:



2. On the user management page, locate the user you need to authorize.
3. Click on the username to enter the user details page, then click **Assign Applications** in the upper left corner, as shown below:



4. In the settings window that appears, click **Assign**, set the User Name, and then click **Save and Go Back>Done** to complete the configuration of Okta user operations. As shown in the figure below:



5. Navigate to the Application Management page, and click on the name of the application you created to access the application details page.
6. In the application details page, select **General**. Copy **Embed Link** under the **App Embed Link** box and log in to the Tencent Cloud console.

Policies
Relevant Concepts

Last updated：2024-01-31 17:36:53

Use Cases

When creating a new sub-user or user group, by default, they have no permissions. The primary account or administrator needs to bind policies to them in order to grant them operation permissions for certain cloud resources.

Permissions and Policies

Permission

Permissions are used to allow or deny specified operations or access to specified resources under specified conditions.
By default, a root account is the resource owner and has full access to all resources under the account, while a sub-account does not have access to any resources. Resource creators does not automatically possess access to resources they created and needs be authorized by the resource owner.

Rule

A policy is a syntax rule used to define and describe one or more permissions.
Tencent Cloud's policy types are divided into preset policies and custom policies. CAM provides various methods to create and manage policies from different perspectives. If you need to add permissions to CAM users or groups, you can directly associate preset policies, or create custom policies and then associate them with CAM users or groups. Each policy can contain multiple permissions, and you can attach multiple policies to a single CAM user or group.

Policy types	Creator	Use Cases	Usage Limits
Preset Policy	Tencent Cloud	Commonly used permissions with high frequency include super administrator and full read-write access to resources.	Users are only permitted to use, but not modify.
Custom Policy	User	Refined permission management. For instance, associating a policy with a database administrator, granting them the authority to manage cloud database instances, but not cloud server instances.	Users have the autonomy to create and manage.

Authorization Guide
Creating Custom Polices through Policy Generator

Last updated：2024-01-31 17:38:56

Scenario

This document provides guidance on how to create custom policies using the policy generator. By selecting services, actions, and defining resources from the policy wizard, policy syntax is automatically generated. This method is highly recommended as it can flexibly meet differentiated permission management needs.

Instructions

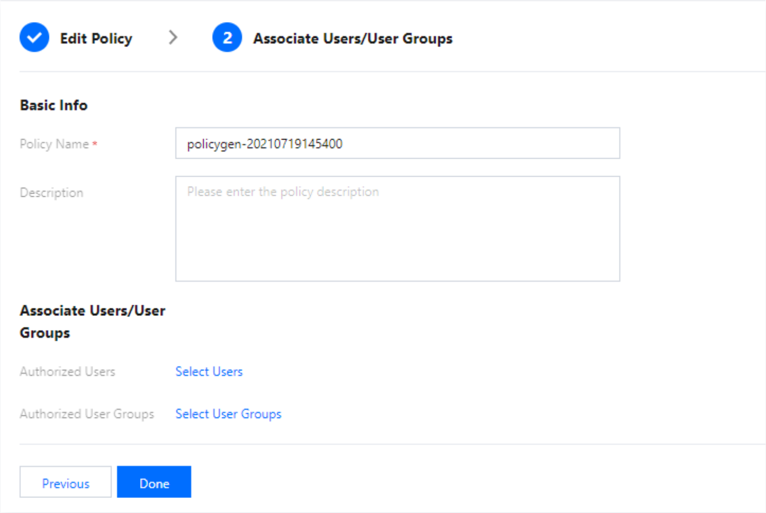
1. On the Policies page of the Cloud Access Management Console, click **Create Custom Policy** in the upper left corner.
2. In the pop-up window for selecting the creation method, click **Create by Policy Generator** to enter the policy editing page.
3. On the "Visual Policy Generator" page for selecting services, provide the following information to edit an authorization statement. (You can also choose JSON and edit the policy using policy syntax. The authorization effect is the same as the "Visual Policy Generator".)
   - Effect (Required): Choose between Allow and Deny.
   - Service (Required): Select the product to be authorized.
   - Action (required): select the actions you want to authorize.
   - Resource (required): Choose all resources or the specific resources you want to authorize.
     For cloud products with operation-level or service-level authorization granularity, it is not necessary to fill in the specific six-segment resource description; simply select all resources.
     For cloud products with resource-level authorization granularity, you can select specific resources. For the resource description method, please see the 'API List' document of the corresponding product in Services Supported by CAM - Overview. For the authorization granularity supported by cloud products, please see 'Authorization Granularity' in Services Supported by CAM - Overview.
   - Condition (optional): Set the conditions under which the above authorization will take effect. For more information, see Effective Conditions.

> **Note**
> - To authorize multiple services, click "Add Permissions" to continue adding multiple authorization statements and configure authorization policies for other services.
> - Multiple statements can be added in one policy.

4. After completing the policy authorization statement editing, click "Next" to proceed to the basic information and associated user/user group/role page.
5. On the Associate User/User Group/Role page, supplement the policy name and description information. You can also quickly authorize by associating users/user groups/roles simultaneously.

> **Note**
> The policy name is automatically generated by the console, with the default prefix "policygen" and a suffix number based on the creation date. You can customize the name as needed.

6. Click **Done** to finish creating a custom policy using the policy generator.



✓ Edit Policy > 2 Associate Users/User Groups

Basic Info

Policy Name *	policygen-20210719145400
Description	Please enter the policy description

Associate Users/User Groups

Authorized Users	Select Users
Authorized User Groups	Select User Groups

Creating Custom Polices through Tag Authorization

Last updated：2024-01-31 17:39:56

Scenario

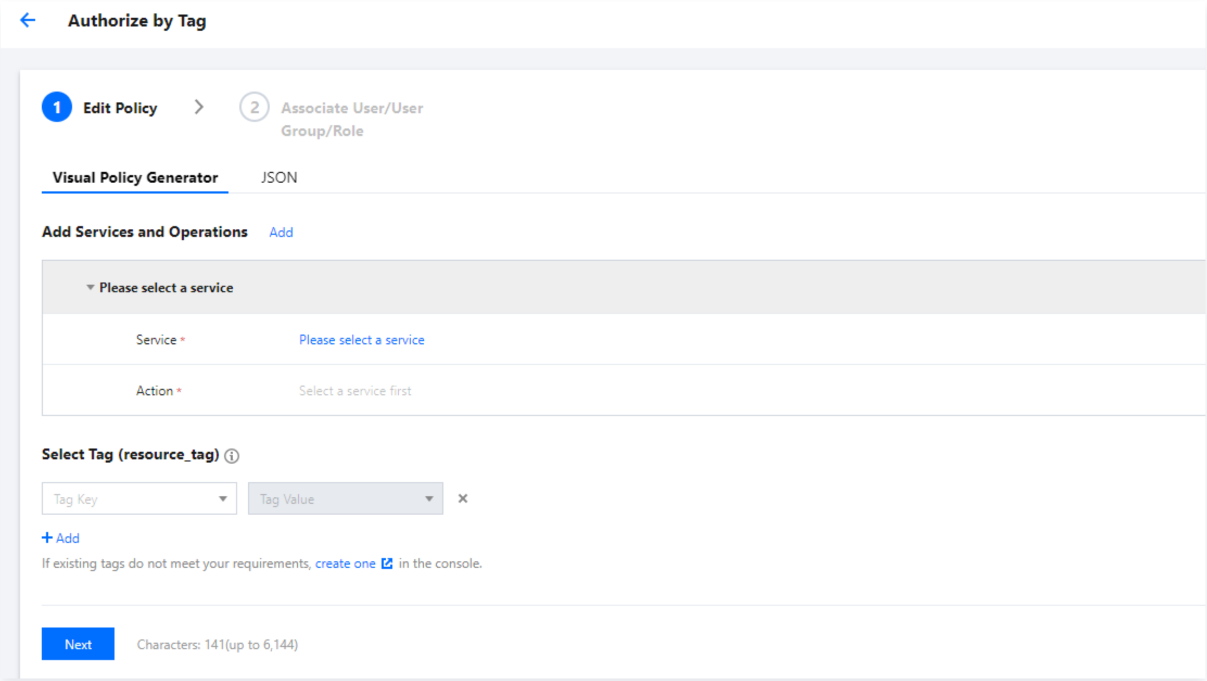
This document outlines how to create a custom policy through tag authorization. Once generated, this policy will have permissions for a category of resources with tag attributes.

Instructions

1. On the Policies page of the Cloud Access Management Console, click **Create Custom Policy** in the upper left corner.
2. In the pop-up window for selecting the creation method, click **Authorize by Tag** to navigate to the page for tag-based authorization.
3. In the service and action addition area of the Visual Policy Generator, enter the following information, and edit an authorization statement.
   - Service (Required): Select the product to be authorized.
   - Action (required): select the actions you want to authorize.

> **Note**
> - The operation includes all interfaces of the service. You can filter and view whether an interface supports tag-based authorization by using the "**Supports Authorization by Tag**" filter.
>   - Yes: Supports tag-based authorization API, which will include operation permissions for resources associated with corresponding tags.
>   - No: The tag-based authorization API is not supported, which will include operation permissions for all resources.
> - To support the authorization of multiple services, click "Add" in the upper left corner to continue adding multiple authorization statements and configure authorization policies for other services.
> - Multiple statements can be added in one policy.

4. In the Select Tag section, choose the tag information that needs to be authorized. You can add multiple tags. Click **Next** to proceed to the Associate User/User Group/Role page.

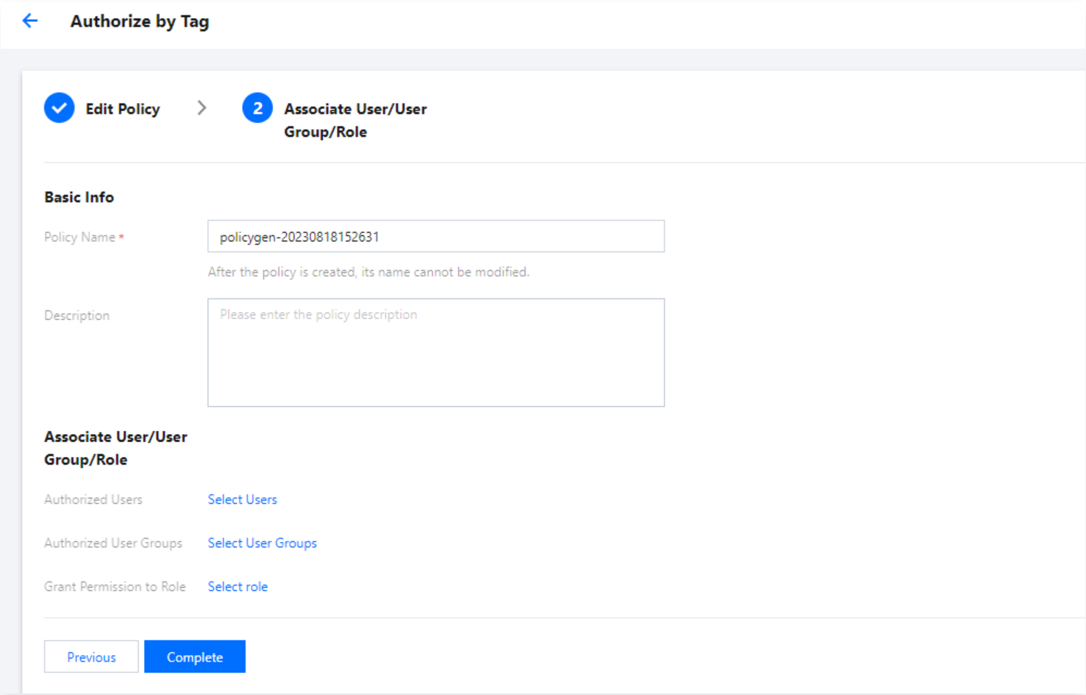

Authorize by Tag
1 Edit Policy
2 Associate User/User Group/Role
Visual Policy Generator
JSON
Add Services and Operations
Add
Please select a service
Service *
Please select a service
Action *
Select a service first
Select Tag (resource_tag)
Tag Key
Tag Value
+ Add
If existing tags do not meet your requirements, create one in the console.
Next
Characters: 141(up to 6,144)

5. On the Associate User/User Group/Role page, supplement the policy name and description information. You can simultaneously associate users/user groups/roles for quick authorization.

Note

The policy name is automatically generated by the console, with the default prefix "policygen" and a suffix number based on the creation date. You can customize the name as needed.

6. Click **Complete** to finish creating a custom policy using the policy generator.



← Authorize by Tag

✓ Edit Policy > 2 Associate User/User Group/Role

Basic Info

Policy Name *: policygen-20230818152631

After the policy is created, its name cannot be modified.

Description: Please enter the policy description

Associate User/User Group/Role

Authorized Users: Select Users

Authorized User Groups: Select User Groups

Grant Permission to Role: Select role

Creating Custom Policies through Policy Syntax

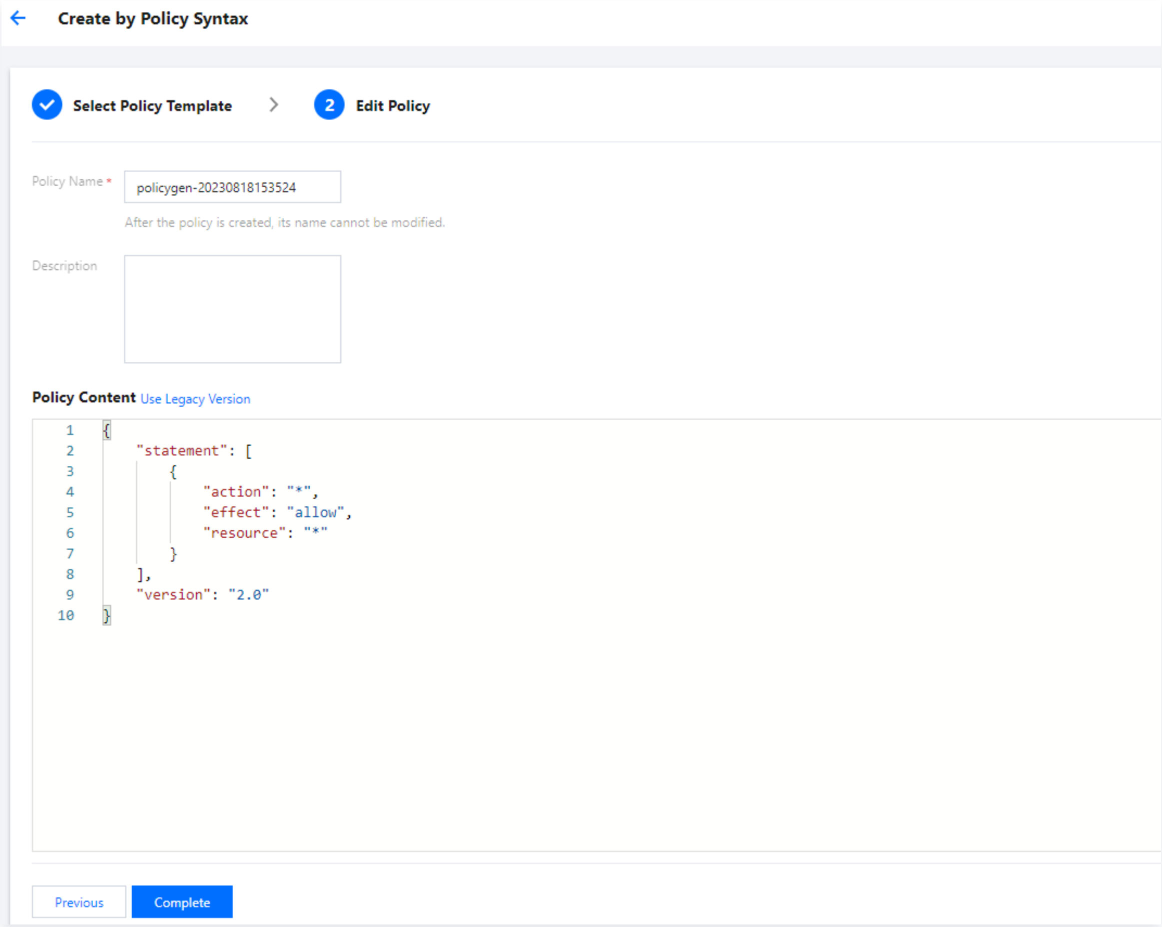
Last updated：2023-08-31 18:20:07

Scenario

This document provides guidance on creating custom policies through policy syntax. This method allows users to write policy syntax, generating corresponding policies with flexible permission granularity. It is particularly useful for users who require a high degree of precision in permission allocation.

Instructions

1. On the Policies page of the Cloud Access Management Console, click **Create Custom Policy** in the upper left corner.
2. In the pop-up window for selecting the creation method, click **Create by Policy Syntax** to proceed to the Select Policy Template page.
3. On the Select Policy Template page, you can enter keywords to search. For instance, if the template type is set to All Templates and the keyword is 'a', you can select the AdministratorAccess template.
4. Click **Next** to proceed to the Edit Policy page.
5. On the Edit Policy page, confirm the policy name and policy content, then click **Complete** to complete the creation of a custom policy using policy syntax. The default policy name and policy content are automatically generated by the console. The default policy name is **policygen**, with a suffix number generated based on the creation date.



Policy Name * policygen-20230818153524

After the policy is created, its name cannot be modified.

Description

Policy Content Use Legacy Version

```
{
    "statement": [
        {
            "action": "*",
            "effect": "allow",
            "resource": "*"
        }
    ],
    "version": "2.0"
}
```

Creating Custom Policies through Product Features or Project Permissions

Last updated：2024-01-31 17:46:52

Scenario

This document provides guidance on how to create custom policies through product features or project permissions. By simply enabling or disabling the corresponding product features or project management functions, the corresponding custom policies will be automatically generated.

Instructions

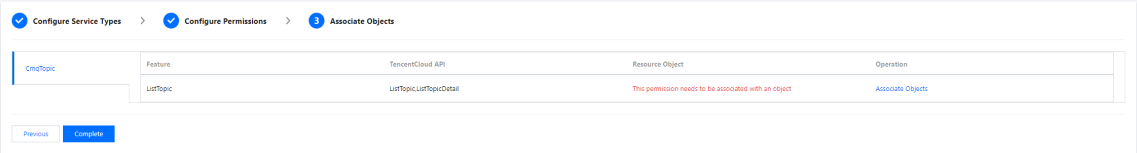
Creating by product feature

With a policy created by product feature, you can control the permission granularity during business access, which helps meet the moderate yet uncomplicated requirements for permission division.

1. On the policy management page, click **Create Custom Policy** in the upper left corner.
2. In the pop-up window for selecting the creation method, click **Create by Product Feature or Project Permission** to navigate to the service type configuration page.
3. On the **Configure Service Types** page, enter the policy name.
4. Select the service type in the **Service Type** column, then click **Next** to proceed to the permission activation page.

> **Note**
> - You can choose from Queue Model, Topic Model, or Content Delivery Network.
> - You can select multiple items.

5. On the permission activation page, set the switch for the required feature permission to **Enabled**, then click **Next** to proceed to the associated object page.
6. On the Associated Objects page, click on **Associate Object** and select the object you wish to associate.
7. Click **Complete** to finish creating a custom policy based on product features.



Feature	TencentCloud API	Resource Object	Operation
ListTopic	ListTopic,ListTopicDetail	This permission needs to be associated with an object	Associate Objects

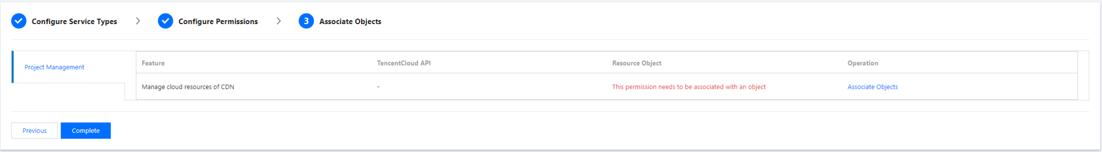
Creating by project permission

Policies created by project permission quickly authorize resources under the same project to a user or user group.

1. On the policy management page, click **Create Custom Policy** in the upper left corner.
2. In the pop-up window for selecting the creation method, click **Create by Product Feature or Project Permission** to navigate to the service type configuration page.
3. On the Configure Service Type page, enter the policy name and select Project Management in the Choose Service Type column. Click **Next** to proceed to the Enable Permissions page.
4. On the **Configure Permissions** page, configure the project management feature according to your actual needs.
   - If you need to manage CDN-related project cloud resources, please set the ○ for "Managing Cloud Resources within CDN Business Projects" to ●.
   - If you need to manage cloud resources related to other product projects, please set the ○ for "Manage Cloud

Resources in Other Business Projects" to ●.

5. On the Associated Objects page, click on "Associate Objects".
6. In the pop-up box for associated objects, select by project, check the objects you want to associate, and click **Confirm**.
7. Click **Complete** to finish creating a custom policy based on project permissions.



Feature	TencentCloud API	Resource Object	Operation
Manage cloud resources of CDN	-	This permission needs to be associated with an object	Associate Objects

Authorization Management

Last updated：2024-01-31 17:51:53

Scenario

When a user or user group is created, they have no permissions by default. You can associate a policy with them to grant them the corresponding operation permissions.

Preparations

- You have created a sub-user / user group.
- If you need to associate a custom policy, please create a custom policy first.

Instructions

You can associate policies with users/user groups and vice versa. These two methods have different operation entries, but they implement the same feature.

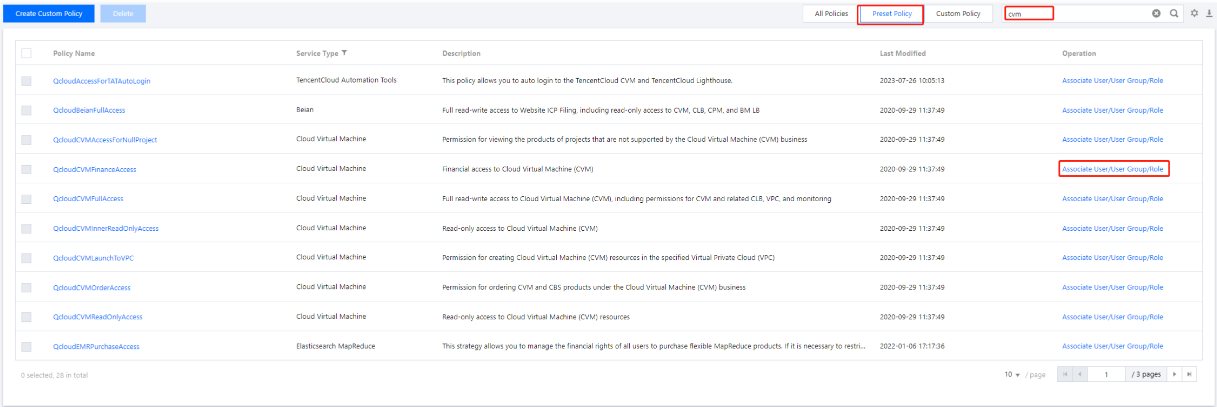
Associating policy with user/user group

Associating Users through Policy

1. On the Policies page of the Cloud Access Management Console, select the policy type.

> **Note**
> This example uses a **preset policy** as a reference, but you can also choose a **custom policy**.

2. Filter the preset policy that needs to be authorized by searching, and click **Associate User/Group/Role** in the operation column.

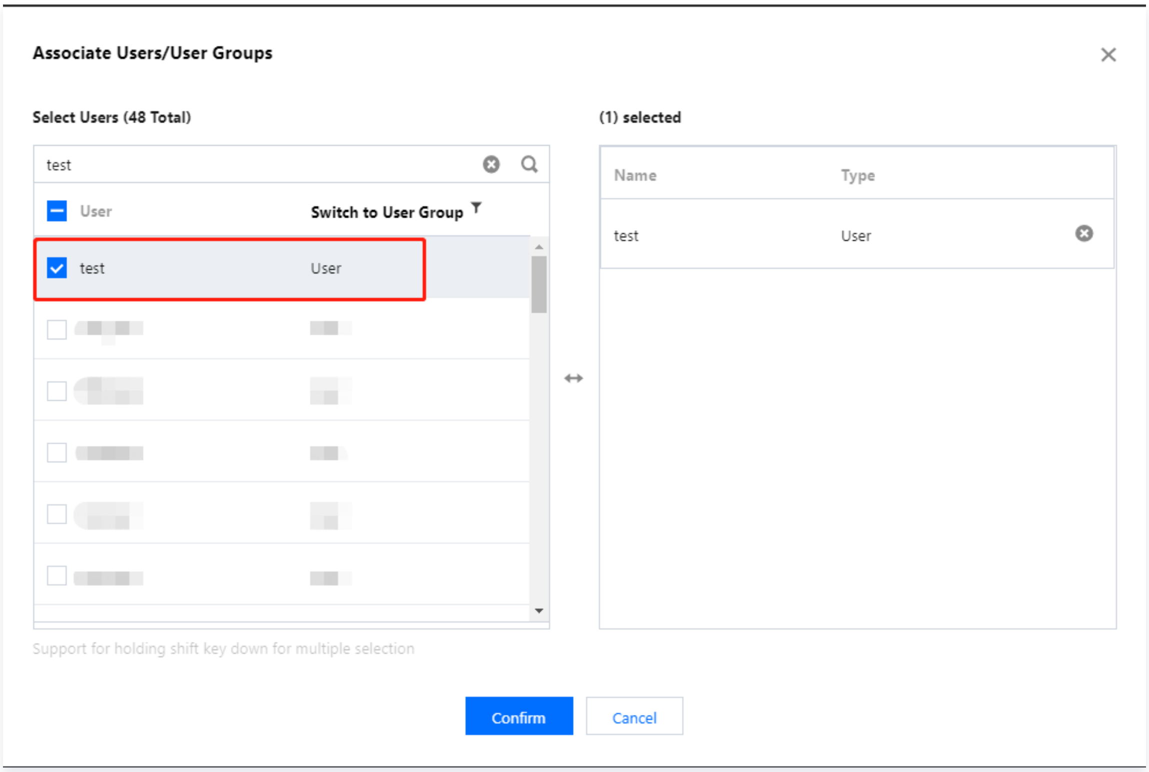


□	Policy Name	Service Type	Description	Last Modified	Operation
□	QcloudAccessForTATAutoLogin	TencentCloud Automation Tools	This policy allows you to auto login to the TencentCloud CVM and TencentCloud Lighthouse.	2023-07-26 10:05:13	Associate User/User Group/Role
□	QcloudBeianFullAccess	Beian	Full read-write access to Website ICP Filing, including read-only access to CVM, CLB, CPM, and BM LB	2020-09-29 11:37:49	Associate User/User Group/Role
□	QcloudCVMAccessForNullProject	Cloud Virtual Machine	Permission for viewing the products of projects that are not supported by the Cloud Virtual Machine (CVM) business	2020-09-29 11:37:49	Associate User/User Group/Role
□	QcloudCVMFinanceAccess	Cloud Virtual Machine	Financial access to Cloud Virtual Machine (CVM)	2020-09-29 11:37:49	Associate User/User Group/Role
□	QcloudCVMFullAccess	Cloud Virtual Machine	Full read-write access to Cloud Virtual Machine (CVM), including permissions for CVM and related CLB, VPC, and monitoring	2020-09-29 11:37:49	Associate User/User Group/Role
□	QcloudCVMInnerReadOnlyAccess	Cloud Virtual Machine	Read-only access to Cloud Virtual Machine (CVM)	2020-09-29 11:37:49	Associate User/User Group/Role
□	QcloudCVMLaunchToVPC	Cloud Virtual Machine	Permission for creating Cloud Virtual Machine (CVM) resources in the specified Virtual Private Cloud (VPC)	2020-09-29 11:37:49	Associate User/User Group/Role
□	QcloudCVMOrderAccess	Cloud Virtual Machine	Permission for ordering CVM and CBS products under the Cloud Virtual Machine (CVM) business	2020-09-29 11:37:49	Associate User/User Group/Role
□	QcloudCVMReadOnlyAccess	Cloud Virtual Machine	Read-only access to Cloud Virtual Machine (CVM) resources	2020-09-29 11:37:49	Associate User/User Group/Role
□	QcloudEMRPurchaseAccess	Elasticsearch MapReduce	This strategy allows you to manage the financial rights of all users to purchase flexible MapReduce products. If it is necessary to restri...	2022-01-06 17:17:36	Associate User/User Group/Role

0 selected, 28 in total

10 / page 1 / 3 pages

3. In the "Associate User/User Group/Role" window that appears, check the users you want to associate and click **Confirm** to complete the operation of associating users through policy.



Associate Users/User Groups

Select Users (48 Total)

(1) selected

test

☐	User	Switch to User Group
☑	test	User

Name	Type
test	User

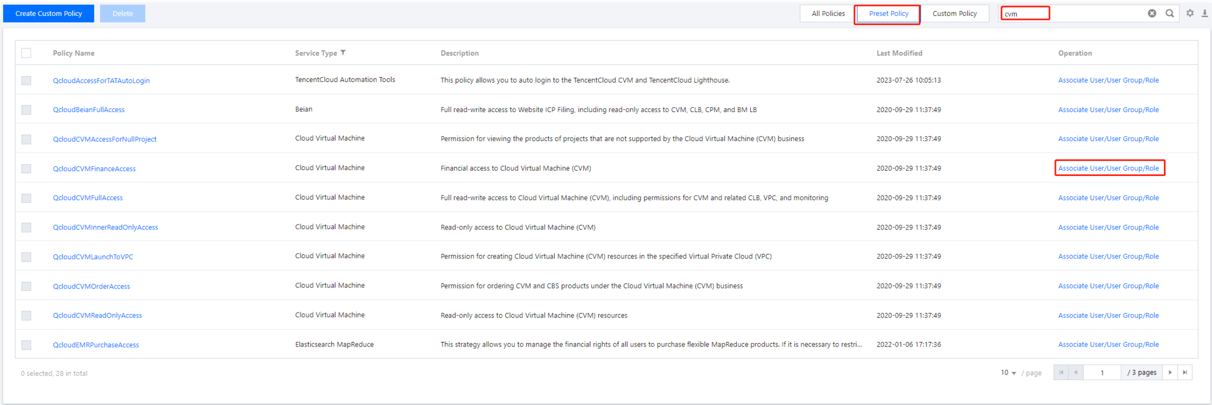
Support for holding shift key down for multiple selection

Associating User Groups through Policy

1. On the Policies page of the Cloud Access Management Console, select the policy type.

> **Note**
> This example uses a **preset policy** as a reference, but you can also choose a **custom policy**.

2. Filter the preset policy that needs to be authorized by searching, and click **Associate User/Group/Role** in the operation column.

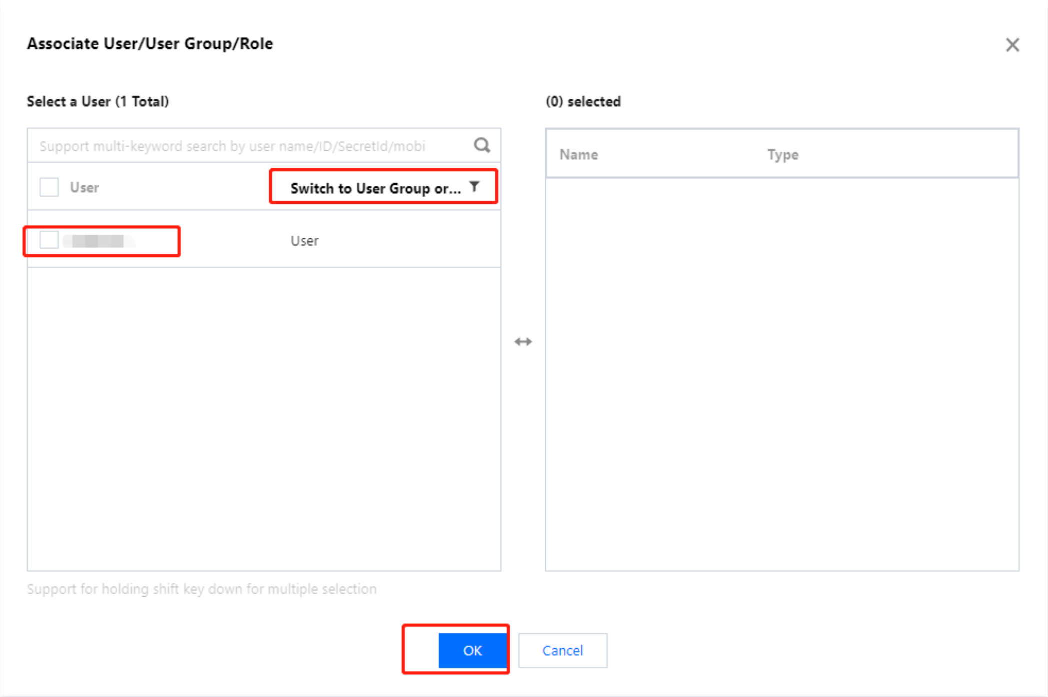


cvm

Policy Name	Service Type	Description	Last Modified	Operation
QcloudAccessForTATAutoLogin	TencentCloud Automation Tools	This policy allows you to auto login to the TencentCloud CVM and TencentCloud Lighthouse.	2023-07-26 10:05:13	Associate User/User Group/Role
QcloudBeianFullAccess	Beian	Full read-write access to Website ICP Filing, including read-only access to CVM, CLB, CPM, and BM LB	2020-09-29 11:37:49	Associate User/User Group/Role
QcloudCVMAccessForNullProject	Cloud Virtual Machine	Permission for viewing the products of projects that are not supported by the Cloud Virtual Machine (CVM) business	2020-09-29 11:37:49	Associate User/User Group/Role
QcloudCVMFinanceAccess	Cloud Virtual Machine	Financial access to Cloud Virtual Machine (CVM)	2020-09-29 11:37:49	Associate User/User Group/Role
QcloudCVMFullAccess	Cloud Virtual Machine	Full read-write access to Cloud Virtual Machine (CVM), including permissions for CVM and related CLB, VPC, and monitoring	2020-09-29 11:37:49	Associate User/User Group/Role
QcloudCVMInnerReadOnlyAccess	Cloud Virtual Machine	Read-only access to Cloud Virtual Machine (CVM)	2020-09-29 11:37:49	Associate User/User Group/Role
QcloudCVMLaunchToVPC	Cloud Virtual Machine	Permission for creating Cloud Virtual Machine (CVM) resources in the specified Virtual Private Cloud (VPC)	2020-09-29 11:37:49	Associate User/User Group/Role
QcloudCVMOrderAccess	Cloud Virtual Machine	Permission for ordering CVM and CBS products under the Cloud Virtual Machine (CVM) business	2020-09-29 11:37:49	Associate User/User Group/Role
QcloudCVMReadOnlyAccess	Cloud Virtual Machine	Read-only access to Cloud Virtual Machine (CVM) resources	2020-09-29 11:37:49	Associate User/User Group/Role
QcloudEMRPurchaseAccess	Elasticsearch MapReduce	This strategy allows you to manage the financial rights of all users to purchase flexible MapReduce products. If it is necessary to restri...	2022-01-06 17:17:36	Associate User/User Group/Role

0 selected, 28 in total

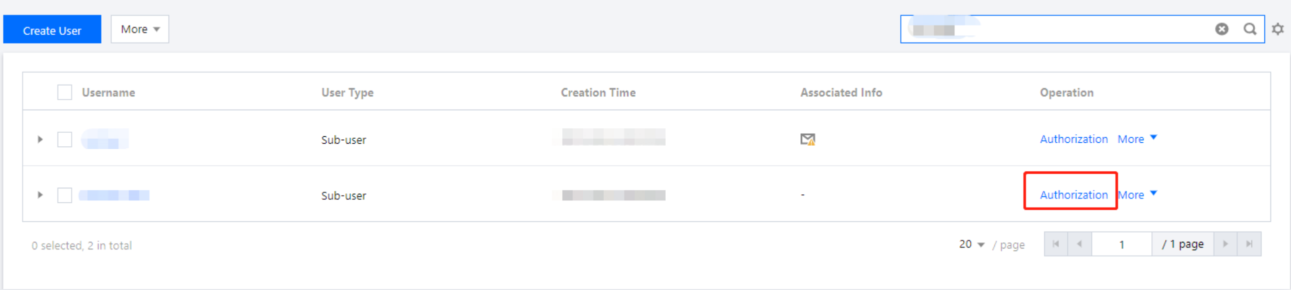
3. In the "Associate User/User Group/Role" window that appears, click **Switch to User Group or Role** and select **User Group**.
4. Select the user group you wish to associate, then click **Confirm** to complete the operation of associating the user group through the policy.


Associate User/User Group/Role
Select a User (1 Total)
Support multi-keyword search by user name/ID/SecretId/mobi
User
Switch to User Group or...
User
(0) selected
Name
Type
Support for holding shift key down for multiple selection
OK
Cancel

Associating user/user group with policy

Associating Policies through Users

1. In the **Users** > User List page of the Cloud Access Management Console, locate the user to be authorized and click **Authorization** in the operation column to enter the policy association page.

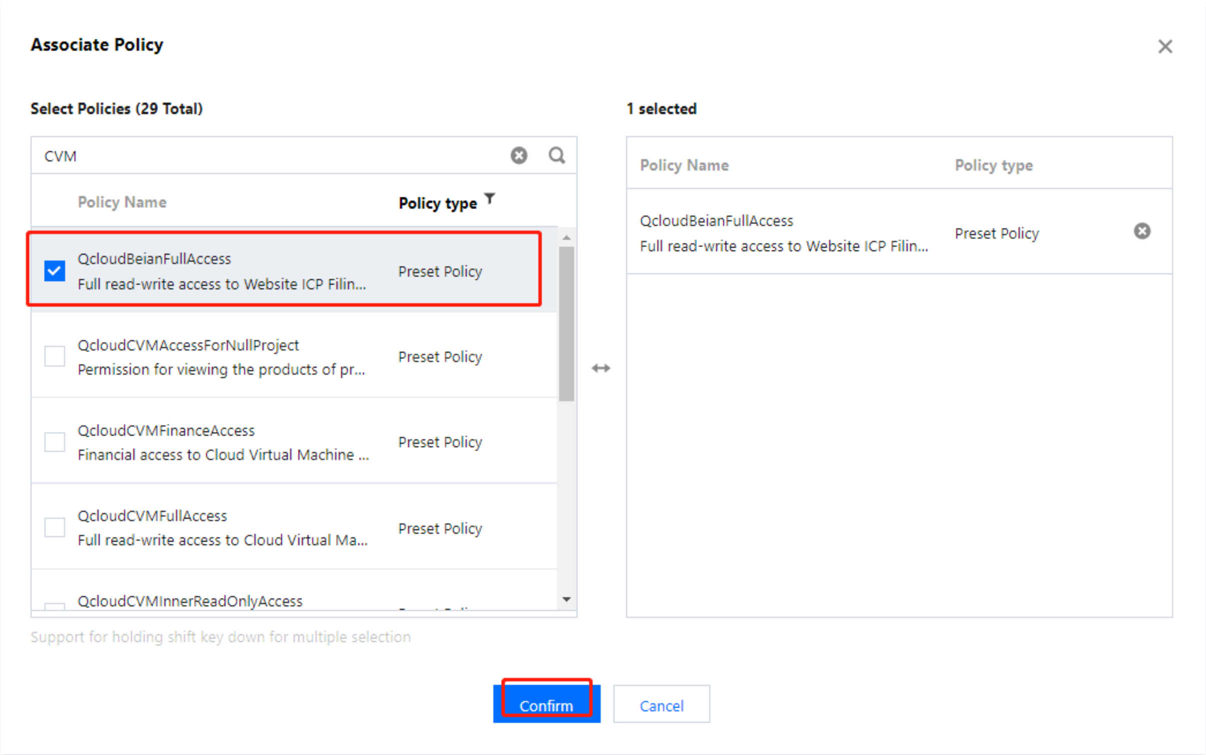


Username	User Type	Creation Time	Associated Info	Operation
	Sub-user			Authorization More
	Sub-user		-	Authorization More

2. On the **Associate Policy** page, select a policy type.

> **Note**
> All policies are displayed by default. You can filter custom or preset policies to find specific policy information.

3. Select the policy that needs to be authorized and click **Confirm** to complete the operation of associating the preset policy with the user.



Associate Policy ✕

Select Policies (29 Total)

CVM

	Policy Name	Policy type
☑	QcloudBeianFullAccess Full read-write access to Website ICP Filin...	Preset Policy
□	QcloudCVMAccessForNullProject Permission for viewing the products of pr...	Preset Policy
□	QcloudCVMFinanceAccess Financial access to Cloud Virtual Machine ...	Preset Policy
□	QcloudCVMFullAccess Full read-write access to Cloud Virtual Ma...	Preset Policy
□	QcloudCVMInnerReadOnlyAccess	

Support for holding shift key down for multiple selection

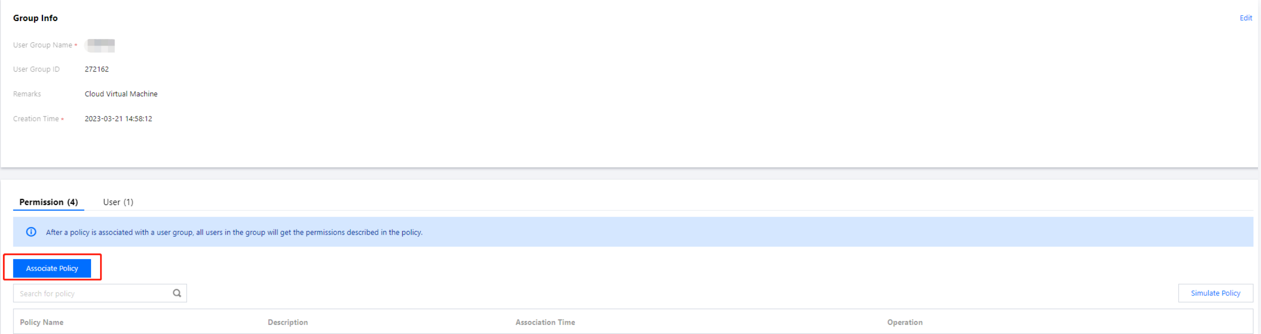
1 selected

Policy Name	Policy type
QcloudBeianFullAccess Full read-write access to Website ICP Filin...	Preset Policy

Confirm　Cancel

Associating Policies through User Groups

1. On the User Group page of the Cloud Access Management Console, click on the target user group name to enter the user group details page.
2. On the user group details page, click **Associate Policy** to navigate to the policy association page.



Group Info　Edit

User Group Name * [redacted]

User Group ID 272162

Remarks Cloud Virtual Machine

Creation Time * 2023-03-21 14:58:12

Permission (4)　User (1)

After a policy is associated with a user group, all users in the group will get the permissions described in the policy.

Associate Policy

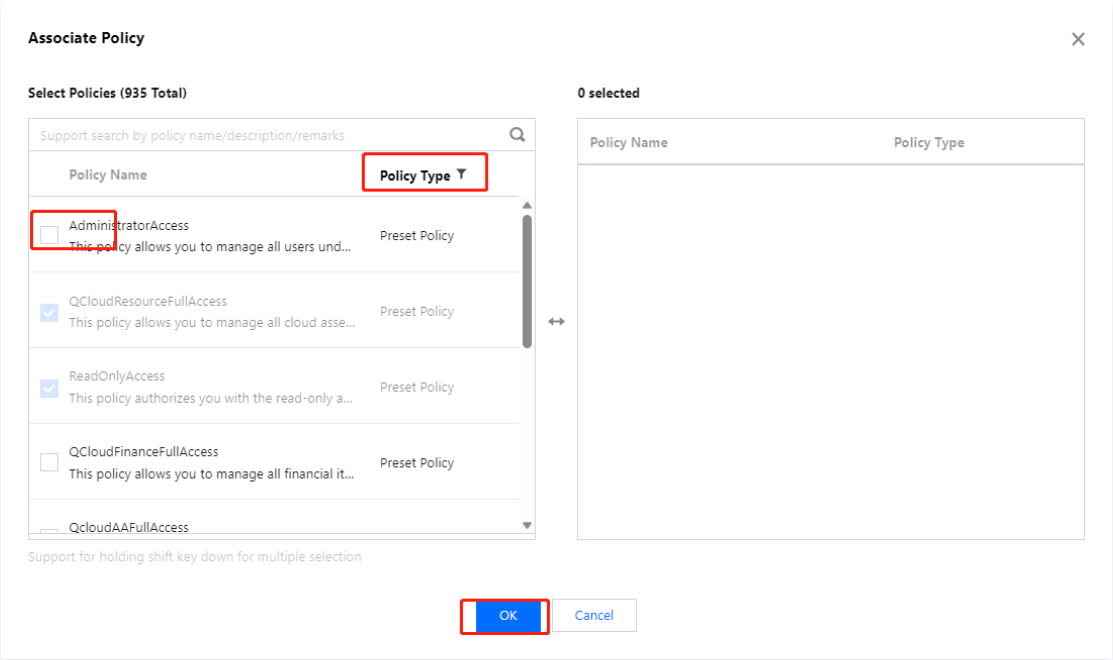
Search for policy　Simulate Policy

Policy Name	Description	Association Time	Operation

3. On the **Associate Policy** page, select a policy type.

> **Note**
> All policies are displayed by default. You can filter custom or preset policies to find specific policy information.

4. Select the policy that needs to be authorized and click **OK** to complete the operation of associating the preset policy with the user.



Associate Policy

Select Policies (935 Total)

Support search by policy name/description/remarks

	Policy Name	Policy Type
□	AdministratorAccess This policy allows you to manage all users und...	Preset Policy
☑	QCloudResourceFullAccess This policy allows you to manage all cloud asse...	Preset Policy
☑	ReadOnlyAccess This policy authorizes you with the read-only a...	Preset Policy
□	QCloudFinanceFullAccess This policy allows you to manage all financial it...	Preset Policy
	QcloudAAFullAccess	

0 selected

Policy Name	Policy Type

Support for holding shift key down for multiple selection

Associated Documents

If you wish to understand the concept of policies, please refer to Policy Definitions.

IP Access Restrictions

Last updated：2024-01-31 17:54:04

Scenario

This document describes how to use custom policy to restrict sub-accounts’ access IPs. After setting the policy, the set IPs will control the sub-accounts’ access to the root account resources.

Preparations

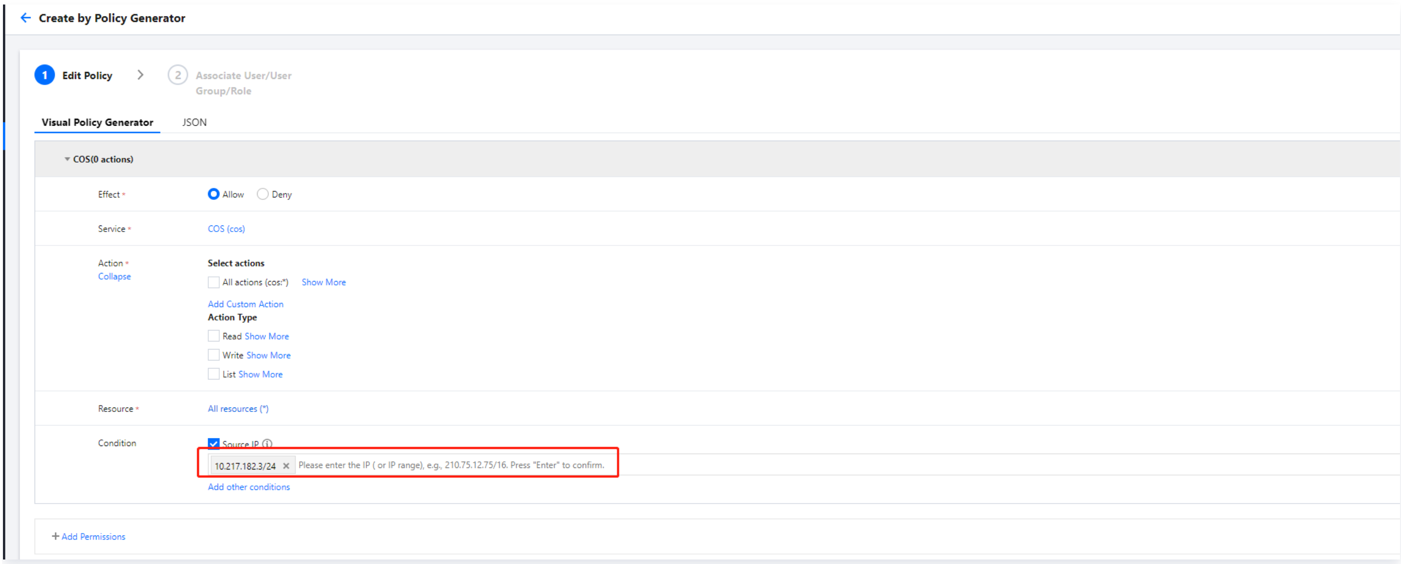
The product you intend to set up must support business access restrictions based on IP. For more information, see Frequently Asked Questions.

Instructions

1. Navigate to the Policy management page and click on **Create Custom Policy** in the upper left corner.
2. In the pop-up window for selecting the creation method, click on **Create by Policy Generator** to proceed to the service and operation selection page.
3. In the Service and Action selection page, enter the following information:
   - Effect: This is a required field. Select "Allow". If "Deny" is selected, the user or user group will not be granted authorization.
   - Service: This is a required field. Select the product you wish to add.
   - Operation: Select the product permissions according to your requirements. This is a mandatory step.
   - Resource: This is a required field. You can see Resource Description Method for guidance.
   - Condition: Choose the condition based on your requirements and enter the IP address. Multiple restrictions can be added. For instance, if "Allow" is selected, only users or groups using this IP address will be granted authorization.

Sample Code

In the following example, the user must be in the 10.217.182.3/24 or 111.21.33.72/24 IP ranges to invoke the cos:PutObject Cloud API call. This is shown in the following figure:



Create by Policy Generator

1 Edit Policy > 2 Associate User/User Group/Role

Visual Policy Generator | JSON

COS(0 actions)

Effect * ● Allow ○ Deny

Service * COS (cos)

Action * Collapse

Select actions

□ All actions (cos:*) Show More

Add Custom Action

Action Type

□ Read Show More

□ Write Show More

□ List Show More

Resource * All resources (*)

Condition ☑ Source IP ⓘ

10.217.182.3/24 × Please enter the IP (or IP range), e.g., 210.75.12.75/16. Press "Enter" to confirm.

Add other conditions

+ Add Permissions

The policy syntax is as follows:

```
{
 "version": "2.0",
 "statement": [
 {
    "effect": "allow",
    "action": "cos:PutObject",
    "resource": "*",
    "condition": {
```

```
    "ip_equal": {
      "qcs:ip": [
        "10.217.182.3/24",
        "111.21.33.72/24"
      ]
    }
  }
}
]
}
```

Syntax Logic
Element Reference

Last updated：2024-01-31 17:54:57

A policy is composed of several elements that describe the specific details of authorization. The core elements include the principal, action, resource, condition, and effect. Element keywords only support lowercase. There is no specific order required in their description. For policies without specific condition constraints, the `condition` element is optional.

1. Version

It describes the version of the policy syntax. This element is required. Currently, only the value "2.0" is permitted.

2. Statement

It describes the details of one or more permissions. This element includes a permission or collection of permissions from several other elements such as `principal` , `action` , `resource` , `condition` , and `effect` . A policy contains only one `statement` element.

3. Principal

It describes the entity authorized by the policy, including users (primary accounts, sub-accounts), and in the future, it will include more entities such as roles and federated identity users. **This element is only supported in the role's trust policy and COS bucket policy.**

4. Action

It describes the allowed or denied operations. An operation can be an API (described with a "name" prefix) or a feature set (a specific set of APIs, described with an "actionName" prefix). This element is required.

```
{
 "version": "2.0",
 "statement": [
  {
   "effect": "allow",
   "action": [
    "ES:CreateServerlessSpace",
    "ES:CreateServerlessInstance",
    "ES:DescribeServerlessInstances",
    "ES:CreateServerlessInstanceUser",
    "ES:DescribeServerlessInstanceUsers",
    "ES:CreateServerlessDi",
    "ES:DescribeServerlessDi",
    "ES:DeleteServerlessInstanceUser",
    "ES:DeleteServerlessDi",
    "ES:DeleteServerlessInstance",
    "ES:DescribeServerlessSpaces",
    "ES:SearchServerlessData"
   ],
   "resource": [
    "*"
   ]
  }
 ]
}
```

5. Resource

It describes the specific data authorized. A resource is described in a six-segment format. Detailed resource definitions vary by product. For more information, please see Resource Description Method. This element is required.

6. Condition

It describes the constraints under which the policy takes effect. Conditions consist of operators, operation keys, and operation values. Condition values can include time and IP address information. Some services allow you to specify other values in the conditions. This element is not required. For more details, see Condition keys and condition operators.

```
{
 "version": "2.0",
 "statement": [
  {
   "effect": "allow",
   "action": [
    "cam:*"
   ],
   "resource": [
    "*"
   ],
   "condition": {
    "ip_equal": {
     "qcs:ip": [
      "10.9.189.79"
     ]
    }
   }
  }
 ]
}
```

7. Effect

It describes whether the result of the statement is "allow" or "explicit deny". It includes two scenarios: `allow` and `deny`. This element is required.

8. Sample Policy

This example describes: granting the sub-account ID (referred to as UIN) 3232523, under the main account APPID (referred to as UID) 1238423, the permission to have all COS read APIs and the authority to write objects, as well as the ability to send message queues, when accessing the object `object2` in the COS bucket `bucketA` in the Beijing region and the COS bucket `bucketB` in the Guangzhou region, from an IP address in the 10.121.2.* range.

```
{
 "version": "2.0",
 "statement": [
  {
   "principal": {
    "qcs": [
     "qcs::cam::uid/1238423:uin/3232523"
    ]
   },
   "effect": "allow",
   "action": [
    "cos:PutObject",
    "cos:GetObject",
    "cos:HeadObject",
    "cos:OptionsObject",
    "cos:ListParts",
    "cos:GetObjectTagging"
   ],
   "resource": [
    "qcs::cos:ap-beijing:uid/1238423:bucketA-1238423/*",
    "qcs::cos:ap-guangzhou:uid/1238423:bucketB-1238423/object2"
   ],
   "condition": {
    "ip_equal": {
     "qcs:ip": "10.121.2.10/24"
    }
   }
  },
  {
   "principal": {
    "qcs": [
     "qcs::cam::uid/1238423:uin/3232523"
    ]
   },
   "effect": "allow",
   "action": "cmqqueue:SendMessage",
   "resource": "*"
  }
 ]
}
```

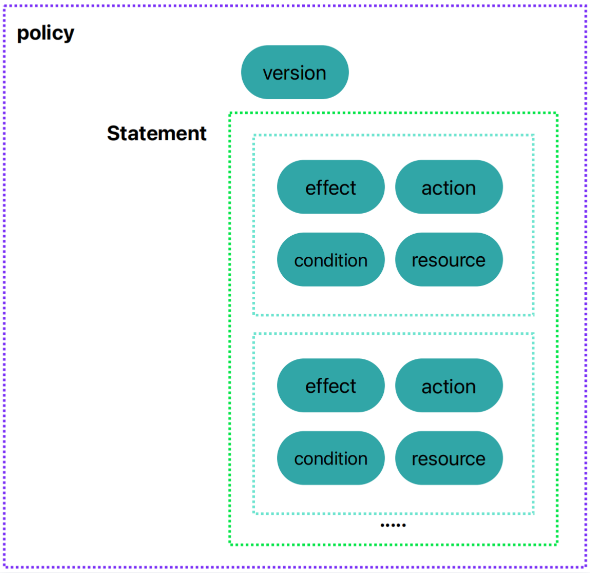
Associated Documents

If you wish to understand the description of CAM resources, please see Resource Description Method.

Syntax Structure

Last updated：2024-01-31 17:56:01

The syntax structure of the entire policy is as depicted in the diagram. The policy is composed of the version and the statement. The statement is made up of several sub-statements. Each sub-statement includes four elements: action, resource, condition, and effect. Among them, the condition and principal information are optional.



JSON Format

The policy syntax is based on the JSON format. If the policy being created or updated does not meet the JSON format, it will not be successfully submitted, so users must ensure the correctness of the JSON format. The JSON format standard is defined in RFC7159. You can also use an online JSON validator to check the policy format.

Syntax Convention

Here we list some syntax conventions:

- The following characters are included in the policy syntax as JSON characters:

```
{ } [ ] " , :
```

- The following characters are used to describe special characters in policy syntax and are not included in the policy:

```
= < > ( ) |
```

- When an element allows multiple values, it is represented with a comma separator and ellipsis. For instance:

```
[<resource_string>, < resource_string>, ...]
<principal_map> = { <principal_map_entry>, <principal_map_entry>, ... }
```

When multiple values are allowed, a single value can also be included. When an element has only one value, the trailing comma must be removed, and the square brackets "[]" are optional. For instance:

```
"resource": [<resource_string>]
"resource": <resource_string>
```

- A question mark (?) following an element indicates that the element is optional. For instance:

```
<condition_block?>
```

- In cases where the element is an enumerated value, the enumerated values are represented by a vertical line "|" and the range of enumerated values is defined by parentheses "()". For instance:

```
("allow" | "deny")
```

- String elements are enclosed in double quotes. For instance:

```
<version_block> = "version" : "2.0"
```

Syntax Description

```
policy  = {
    <version_block>
    <principal_block?>,
    <statement_block>
}

<version_block> = "version" : "2.0"

<statement_block> = "statement" : [ <statement>, <statement>, ... ]

<statement> = {
   <effect_block>,
   <action_block>,
   <resource_block>,
   <condition_block?>
}

<effect_block> = "effect" : ("allow" | "deny")

<principal_block> = "principal": ("*" | <principal_map>)

<principal_map> = { <principal_map_entry>, <principal_map_entry>, ... }

<principal_map_entry> = "qcs":
   [<principal_id_string>, <principal_id_string>, ...]

<action_block> = "action":
   ("*" | [<action_string>, <action_string>, ...])

<resource_block> = "resource":
   ("*" | [<resource_string>, <resource_string>, ...])

<condition_block> = "condition" : { <condition_map> }
<condition_map> {
 <condition_type_string> : { <condition_key_string> : <condition_value_list> },
 <condition_type_string> : { <condition_key_string> : <condition_value_list> }, ...
}
<condition_value_list> = [<condition_value>, <condition_value>, ...]
<condition_value> = ("string" | "number")
```

Syntax Description:

- A policy can contain multiple statements.
  The maximum length of a policy is 6,144 characters (excluding spaces). For more information, please refer to Limitations.
  There is no restriction on the display order of each block. For example, in a policy, the `version_block` can follow the `effect_block`, and so on.
- The currently supported syntax version is 2.0.
- The principal_block element is only supported for use in the trust policy of a role and the bucket policy of COS.

- Both action and resource support lists.
- The condition can be a single condition, or a logical combination of multiple sub-condition blocks. Each condition includes a condition operator (condition_type), a condition key (condition_key), and a condition value (condition_value).
- Each statement's effect can be either "deny" or "allow". When a policy contains both "allow" and "deny" statements, the "deny" takes precedence.

String Description

The element strings described in the syntax are as detailed below:

action_string

It consists of description scope, service type, and operation name.

```
// All actions across all products
"action":"*"
"action":":"
// All operations in COS
"action":"cos:*"
// Operation named  GetBucketPolicy  in COS
"action":"cos:GetBucketPolicy"
// Operation for matching some buckets in COS
"action":"cos:Bucket"
// Operation list named  GetBucketPolicy\PutBucketPolicy\DeleteBucketPolicy  in COS
"action":["cos:GetBucketPolicy","cos:PutBucketPolicy","cos: DeleteBucketPolicy"]
```

resource_string

Resource is described in a six-segment format.

```
qcs: project :serviceType:region:account:resource
```

Below is a sample:

```
// The object resource of the COS product, located in the Shanghai region, the resource owner's uid is 10001234, and the resource name is bucket1/object2.
qcs::cos:ap-shanghai:uid/10001234:bucket1-10001234/object2
// CMQ queue. Region: Shanghai. Resource owner uin: 12345678. Resource name: 12345678/queueName1. Resource prefix: queueName
qcs::cmqqueue:sh:uin/12345678:queueName/12345678/queueName1
// CVM instance. Region: Shanghai. Resource owner uin: 12345678. Resource name: ins-abcdefg. Resource prefix: instance
qcs::cvm:sh:uin/12345678:instance/ins-abcdefg
```

If you intend to understand the resource definition details corresponding to each product, please see the reference documentation of the corresponding product in Products Supported by CAM .

condition_type_string

Condition operators describe the type of test conditions. For instance, string_equal, string_not_equal, date_equal, date_not_equal, ip_equal, ip_not_equal, numeric_equal, numeric_not_equal, and so on. Here are some examples:

```
"condition":{
        "string_equal":{"cvm:region":["sh","gz"]},
        "ip_equal":{"qcs:ip":"10.131.12.12/24"}
}
```

condition_key_string

Condition keys denote the values that will be manipulated using conditional operators to determine whether the condition is met. CAM has defined a set of condition keys that can be used across all products, including qcs:current_time, qcs:ip, qcs:uin, and qcs:owner_uin, etc. For more information, please see Effective Conditions.

principal_id_string

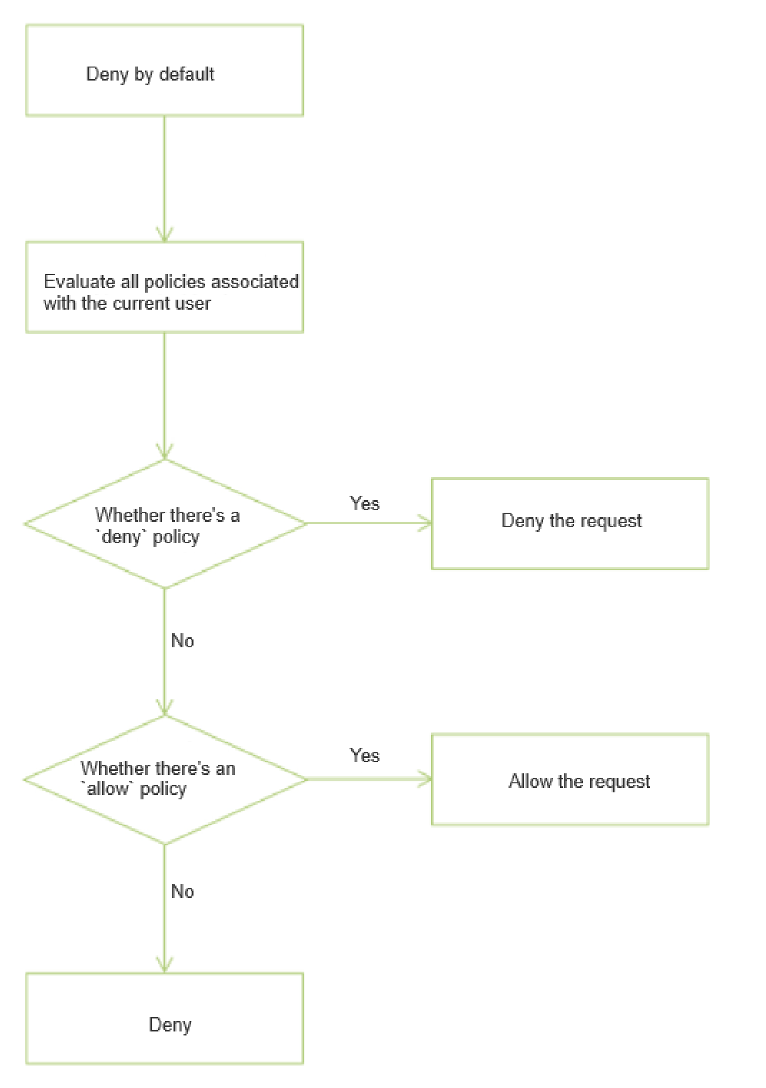
For CAM, users are also considered resources. Therefore, the principal is also described in a six-segment format. For specific information, please see Resource Description Method.

```
"principal":  {"qcs":["qcs::cam::uin/1238423:uin/3232",
        "qcs::cam::uin/1238423:groupid/13"]}
```

Evaluation Logic

Last updated：2024-01-31 17:57:54

When a Tencent Cloud user accesses cloud resources, CAM determines whether to allow or deny the request by using the following evaluation logic.


Deny by default
Evaluate all policies associated with the current user
Whether there's a `deny` policy
Yes
Deny the request
No
Whether there's an `allow` policy
Yes
Allow the request
No
Deny

1. All requests are denied by default.
2. CAM checks all policies currently associated the user.
   2.1 If a policy matches, it proceeds to the next step; otherwise, the final decision is to deny access to the cloud resources.
   2.2 It determines whether any "deny" policies match. If yes, the final result is "deny", and access to cloud resources is not permitted. If no, proceed to the next step.
   2.3 It determines whether any "allow" policies match. If yes, the final result is "allow", and access to cloud resources is permitted. If no, the final result is "deny", and access to cloud resources is not permitted.

⚠ **Note**

- For the primary account, it has default access to all resources under its name; currently, only COS/CAS products support cross-account resource access.
- Certain universal policies are associated with all CAM users by default. For more details, please see the Universal Policy Table below.
- All other policies, including "allow" and "deny", must be explicitly specified.
- For services that support cross-account resource access, there are scenarios of permission delegation, where the

> primary account A authorizes a sub-account under primary account B to access its resources. In this case, CAM will verify both whether A has granted this permission to B and whether B has granted this permission to the sub-account. Only when both conditions are met, the sub-account of B is entitled to access the resources of A.

The table below shows the currently supported general policies:

Policy description	Policy Definition

Query the key requires MFA verification.	{
	"principal":"",
	"action":"account:QueryKeyBySecretId",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

Set sensitive operations to require MFA verification.	{
	"principal":"",
	"action":"account:SetSafeAuthFlag",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

Bind a token requires MFA verification.	{
	"principal":"",
	"action":"account:BindToken",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

Unbind a token requires MFA verification.	{
	"principal":"",
	"action":"account:UnbindToken",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

Modifying the email requires MFA verification.	{
	"principal":"",
	"action":"account:ModifyMail",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

Changing the phone number requires MFA verification.	{
	"principal":"",
	"action":"account:ModifyPhoneNum",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

Resource Description Method

Last updated：2024-01-31 18:00:14

The "resource" element describes one or more objects of operation, such as CVM resources, COS buckets, etc. This document primarily introduces the resource description information of CAM.

Definition of All Resources

- When the "resource" is set to `*`, it represents all resources, thereby granting operation permissions for all resources associated with the action.
- If the authorized cloud service's authorization granularity is at the service level, or if the operation action of the authorized service supports interface-level granularity, the "resource" must be set to *, thereby granting all resource permissions for that cloud service or the service operation action.

Definition of One or Multiple Resources

You can describe the permissions of one or multiple resources in the following six-segment format for authorization. Each service has its own resources and detailed resource definition.
The six-segment format is defined as follows:

```
qcs:project_id:service_type:region:account:resource
```

A six-segment resource description contains six fields as detailed below:

Field	Description and Values	Required	Sample
qcs	The abbreviation for qcloud service, indicating it is a cloud resource of Tencent Cloud.	Supported	qcs
project_id	Describing project information is only compatible with early CAM logic. The current policy syntax prohibits filling in this information, so it can be left blank.	Not required	Set to Null
service_type	• Describes the product's abbreviation. For details, see "Abbreviation in CAM" in Products Supported by CAM. • When the value is null, it represents all products.	Not required	• Cloud Virtual Machine is referred to as CVM. • Content Delivery Network is referred to as CDN.
region	To describe region information, please see the Region List for the naming convention of regions. When the value is empty, it represents all regions.	Not required	• North China (Beijing) is represented as ap-beijing • South China (Guangzhou) is ap-guangzhou
account	Describes the primary account information of the resource owner, currently supporting two methods of description, namely, the uin and uid methods. The uin method refers to the account ID of the primary account, represented as `uin/${uin}`. • The uid method, which is the APPID of the primary account, is represented as `uid/${appid}`. Only the resource owners of COS and CAS services use this method of description. • When the value is empty, it represents the primary account to which the CAM user creating the policy belongs.	Not required	• UIN, for example: `uin/12345678` • uid, for instance: uid/10001234
resource	The detailed resource information of each product is described, currently supporting two ways to describe resource information,	Supported	• Cloud Virtual Machine: instance/ins-1 • TencentDB for MySQL:

	`resource_type/${resourceid}` and `<resource_type>/<resource_path>` . - `resource_type/${resourceid}: resourcetype` is the resource prefix, describing the resource type. For details, see the six-segment resource description of the product in Business Interfaces Supporting CAM . ${resourceid} is the specific resource ID, which can be viewed in each product's console. When the value is `*` , it represents all resources of that type. - `<resource_type>/<resource_path>` : The "resource_type" is a resource prefix that describes the type of resource. - `<resource_path>` is the resource path, which supports directory-level prefix matching. For details, see the six-segment resource format of the product in Business Interfaces Supporting CAM .		instanceId/cdb-1 - Cloud Object Storage (COS): prefix//10001234/bucket1/* represents all files under bucket1. COS resources (resource) support various types. For more details, please see the COS Authorization Policy Usage Guide .

Definition of CAM Resources

CAM resources include users, user groups, and policies. A CAM resource can be described as follows:

Primary Account:

```
qcs::cam::uin/164256472:uin/164256472
```

OR

```
qcs::cam::uin/164256472:root
```

Sub-account:

```
qcs::cam::uin/164256472:uin/73829520
```

Group:

```
qcs::cam::uin/164256472:groupid/2340
```

All resources

```
*
```

Policy:

```
qcs::cam::uin/12345678:policy/*
```

OR

```
qcs::cam::uin/12345678:policy/12423
```

Notes on Resources

- The owner of a resource is always the primary account. If a resource is created by a sub-account, it will not automatically have access to the resource without authorization. The resource owner must grant access.
- Services such as COS and CAS support cross-account authorization for resource access. The authorized account can delegate resource permissions to its sub-accounts through permission propagation.

Associated Documents

If you wish to understand the detailed resource definitions for each product, please refer to the reference documents for the corresponding products in Products Supported by CAM .

Policy Variable

Last updated：2024-02-01 18:26:40

Use Cases

Scenario Assumption: You wish to grant each CAM user the access rights to the resources they create. For instance, you want to set it such that the creator of a COS resource automatically has access rights to that resource.
If the resource owner (primary account) were to individually authorize each resource to its creator, the authorization cost would be high, requiring a policy to be written and authorized for each type of resource. In this case, you can meet your needs by using policy variables. Add a placeholder in the resource definition of the policy to describe the sub-account uin of the creator, which is the policy variable. During authentication, the policy variable will be replaced with context information from the request itself.
The policy for granting resource access permissions to a creator is described as follows:

```
{
  "version":"2.0",
  "statement": [
    {
      "effect":"allow",
      "action": "cmqqueue:*",
      "resource": "qcs::cmqqueue::uin/1000001:queueName/uin/${uin}/*"
    }
  ]
}
```

- The policy variable includes the sub-account uin of the creator in the path of each resource. For example, if a sub-account with uin 125000000 (corresponding to the main account uin 1000001) creates a CMQ message queue named queueName/uin/125000000 in the Chengdu region, the corresponding resource description would be:

```
qcs::cmqqueue:ap-chengdu:uin/1000001:queueName/uin/125000000
```

- When a sub-account with uin 125000000 accesses this resource, the placeholder in the corresponding policy information will be replaced with the visitor during the authentication process, that is:

```
qcs::cmqqueue::uin/1000001:queueName/uin/125000000
```

- The resource `qcs::cmqqueue::uin/1000001:queueName/uin/125000000` in the policy can access the resource `qcs::cmqqueue:ap-chengdu:uin/1000001:queueName/uin/125000000` through prefix matching.

Location of Policy Variable

Resource Element Position: Policy variables can be used in the last segment of the six-segment resource description.
Condition Element Position: Policy variables can be used in condition values.
The following policy indicates that the VPC creator has the access permission:

```
{
    "version":"2.0",
    "statement": [
     {
      "effect":"allow",
      "action":"name/vpc:*",
      "resource":"qcs::vpc::uin/12357:vpc/*",
      "condition":{"string_equal":{"qcs:create_uin":"${uin}"}}
     }
   ]
}
```

Note
The six-segment resource format for Cloud Object Storage (COS) is `qcs::cos:$region:uid/$appid:$bucketname-$appid/$ResourcesPath` , where $ResourcesPath is the specific resource path, and

> the above policy variable cannot be used in $ResourcesPath. The complete six-segment resource format for a COS bucket is as follows: `qcs::cos:ap-guangzhou:uid/1250000000:examplebucket-1250000000/path_1/path_2/pic.jpeg` .

Policy Variable List

Below is a list of supported policy variables:

Variable	Variable Meaning
${uin}	The current visitor's sub-account uin. In the case where the visitor is the primary account, it is consistent with the primary account uin.
${qcs:user}	The username of the current visitor's sub-account.
${owner_uin}	The uin of the primary account to which the current visitor belongs.
${app_id}	The APPID of the primary account to which the current visitor belongs.

Conditions

Overview of Effective Conditions

Last updated：2024-02-01 18:31:41

When setting up access management policies, you can specify the conditions (Condition) under which the policy takes effect. These conditions are optional. Once set, when a user sends a request to Tencent Cloud, the system will match the condition keys and values in the request context with those specified in the policy. Only when the conditions are successfully matched will the corresponding permission policy take effect.

Composition of Effective Conditions

Effective conditions are composed of one or more condition clauses. A condition clause consists of a condition key, an operator, and a condition value. A single condition key can specify one or more condition values.
`"condition" : { "{condition-operator}" : { "{condition-key}" : "{condition-value}" }}`

Example of a Condition Clause

The request IP is `192.168.1.1` , and the request date is before 2022-05-31 00:00:00. The Condition is as follows:

```
"condition":{
        "ip_equal": {
          "qcs:ip": "192.168.1.1"
        },

        "date_less_than": {
          "qcs:current_time": "2022-05-31 00:00:00"
        }
      }
```

Matching Logic for Activation Conditions

The evaluation logic for effective conditions is as follows:

Evaluation Logic	Note
Condition Satisfaction	A single condition key can specify one or more condition values. During condition checking, if the value of the condition key matches any of the specified values, the condition is deemed to be met.
Condition Clause Fulfillment	Under a condition clause with the same condition operation type, if there are multiple condition keys, all condition keys must be satisfied simultaneously for the condition clause to be deemed fulfilled.
Condition Block Fulfillment	The condition block is only considered satisfied when all condition clauses within it are met simultaneously.
Condition operators (excluding null_equal) with the suffix if_exist	This implies that the context information remains effective even if it does not contain the corresponding key-value pair.
for_all_value	Qualifiers are used in conjunction with condition operators, indicating that the policy will only take effect when each condition value in the context information meets the requirements.
for_any_value	Qualifiers are used in conjunction with condition operators to indicate that any one of the condition values in the context information can satisfy the requirement for the condition key to take effect.

Note

> Authorization by tag only supports 'for_any_value'. For more information on authorizing by tag, please see Manage Project Resources Based on Tags.

Condition Example

```
"condition":{
        "ip_equal": {
          "qcs:ip": "192.168.1.1"
        }
      }
```

The condition value in the request is represented by the condition key, which in this example is qcs:ip. The context key value is compared with the value you specified as a text value, such as `192.168.1.1`. The type of comparison to be performed is specified by the condition operator (here it is ip_equal).

In certain scenarios, it is necessary to match multiple access situations to meet practical needs. In such cases, you can specify multiple condition values when setting the Condition. For instance, the user must be within the `10.217.182.3/24` or `111.21.33.72/24` subnet to upload objects (cos:PutObject). The content of the permission policy is as follows:

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "cos:PutObject"
      ],
      "resource": [
        "*"
      ],
      "condition":{
        "ip_equal": {
          "qcs:ip": [
            "10.217.182.3/24",
            "111.21.33.72/24"
          ]
        }
      }
    }
  ]
}
```

Condition Keys and Condition Operators

Last updated：2023-08-31 18:28:21

When creating a policy through the Cloud Access Management Console's Policy Generator, you can set the policy's effective conditions as needed.

Condition keys

The naming format for Tencent Cloud's universal condition keys is: `qcs:<condition-key>` . Currently, only five condition keys are supported. The content and descriptions of these keys are as follows:

Universal Condition Keys	Local Disk Types	Description
qcs:current_time	Date and time	The time when the Web Server receives a request. This is represented in the ISO8601 standard and must use UTC time.
qcs:ip	IP address	The IP address from which the request is initiated. It must comply with CIDR standards.
qcs:mfa	Boolean	Whether multi-factor authentication was used during user login.
qcs:resource_tag	String	Control access to resources based on the tags attached to them. The policy's specified tag key/value pairs can be compared with the key/value pairs bound to the resource, and the resource can only be accessed when a match is found.
qcs:request_tag	String	Controls which tags can be passed in a request. The policy can compare the specified tag key/value pairs with the key/value pairs passed in the request. Tags can only be bound or unbound when they match.

⚠ Note

- The current condition key can be applied to both global services and specific services.
- Condition keys are case sensitive.

Operator

In the application condition (Condition), use condition operators to match the condition keys and values in the policy with the values in the request context.
Condition operators are divided into seven categories according to their types: String, Number, Date and Time, Boolean, IP Address, Binary, and Null.

Condition Operator Types	Conditional Operators	Description
String Condition Operators	string_equal	String equals (case-sensitive)
	string_not_equal	String is not equal to (case-sensitive)
	string_equal_ignore_case	String equals (case insensitive)
	string_not_equal_ignore_case	String is not equal to (case insensitive)
Numeric Condition Operators	numeric_equal	Number equal to
	numeric_not_equal	Value is not equal to
	numeric_less_than	Less than
	numeric_less_than_equal	Value is less than or equal to
	numeric_greater_than	Greater than or equal to
	numeric_greater_than_equal	Value is greater than or equal to
Date Condition Operators	date_equal	The date and time is equal to

	date_not_equal	The date and time is not equal to
	date_less_than	Date and Time Less Than
	date_less_than_equal	Date and time less than or equal to
	date_greater_than	Date and Time Greater Than
	date_greater_than_equal	Date and time greater than or equal to
Boolean Condition Operators	bool_equal	Boolean Value Matching
Binary Condition Operators	binary_equal	Number equal to
IP Address Condition Operators	ip_equal	IP Address Equals
	ip_not_equal	IP address is not equal to
Empty Condition Key Operators	null_equal	Empty Condition Key Matching

Mapping Relationship

In the effective statement, the conditions (Condition) that can be used depend on the selected condition key. The mapping relationship between the condition key and the operator is as follows:

> **Note**
> The condition values corresponding to the operators string_like and string_not_like only support `uppercase and lowercase letters` , `numbers` , `-` , and `_` , and do not support list-type interfaces. List-type interfaces can be queried through business interfaces that support CAM .

Condition keys	Operator
qcs:resource_tagqcs:request_tag	string_equal
	string_not_equal
	string_equal_ignore_case
	string_not_equal_ignore_case
	string_like
	string_not_like
qcs:current_time	date_equal
	date_not_equal
	date_less_than
	date_less_than_equal
	date_greater_than
	date_greater_than_equal
qcs:ip	ip_equal
	ip_not_equal

Scenarios

Last updated：2023-08-31 18:28:40

Scenario	Description	Sample
The condition operator includes a condition value of a condition key.	Permits the VPC to bind with the specified peering connection, the region of the VPC must be specified.	Example
	Only cloud server instances with bound tags can be restarted.	Example
The condition operator encompasses multiple condition values of a single condition key.	Allow access for users with two specified IP addresses.	Example
Scenarios with multiple condition operators.	Allow access for users with a specified IP and date.	Example
A single condition operator contains multiple condition keys.	Attaching multiple condition keys to a single condition operator would result in	Example
Application of Boolean Condition Operators	Sub-users must bind the token before they can delete the API key.	Example

The condition operator includes a condition value of a condition key.

Description 1

When a CAM user invokes the VPC peering connection API, it is necessary not only to determine whether the CAM user has access permissions for the peering connection API and peering connection resources, but also to confirm whether the CAM user has access permissions for the VPC associated with the peering connection.

Sample Code 1

In the following example, the VPC region must be `Shanghai` in order for it to be bound to a specified peering connection:

```
{
  "version": "2.0",
  "statement": [
  {
    "effect": "allow",
    "action": "name/vpc:AcceptVpcPeeringConnection",
    "resource": "qcs::vpc:sh::pcx/2341",
    "condition": {
      "string_equal_if_exist": {
        "vpc:region": "sh"
      }
    }
  }
 ]
}
```

Description 2

When a CAM user accesses Tencent Cloud resources, it is necessary to restrict the user to only access resources bound with specific tags.

Sample Code 2

The following example describes that users can only restart (cvm:RebootInstances) the cloud server instances bound with the tag "Department & Research and Development".

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "cvm:RebootInstances"
      ],
      "resource": "*",
      "condition": {
        "for_any_value:string_equal": {
          "qcs:resource_tag": [
            "Department&Research and Development"
          ]
        }
      }
    }
  ]
}
```

The condition operator encompasses multiple condition values of a single condition key.

Description

A single condition operator that includes multiple condition values of a condition key is evaluated using the logical OR operator. When there are multiple condition values, a set operator symbol must be used to represent them.
When a CAM user invokes a cloud API, if there is a need to restrict the user's access source, it is required to add an IP condition on the basis of the existing policy.

Sample Code

The following example stipulates that users must be within the `10.217.182.3/24` or `111.21.33.72/24` IP range to upload objects (cos:PutObject).

```
{
  "version": "2.0",
  "statement": [
  {
    "effect": "allow",
    "action": "cos:PutObject",
    "resource": "*",
    "condition": {
      "ip_equal": {
        "qcs:ip": [
          "10.217.182.3/24",
          "111.21.33.72/24"
        ]
      }
    }
  }
 ]
}
```

Scenarios with multiple condition operators.

Description

If your policy has multiple condition operators, they are evaluated using the logical AND.

Sample Code

The following example describes that the user must request IP `192.168.1.1` , and the request date must be earlier than 2022-05-31 00:00:00 to match.

```
"condition": {
        "ip_equal": {
          "qcs:ip": "192.168.1.1"
        },
        "date_less_than": {
          "qcs:current_time": "2022-05-31 00:00:00"
        }
      }
```

A single condition operator contains multiple condition keys.

Description

If your policy has multiple condition operators or attaches multiple condition keys to a single condition operator, then the conditions are evaluated using a logical AND.

Sample Code

The following example describes that the resource tag is "Department & Research and Development", and only when the request tag is "Department & Research and Development" can it be matched.

```
"condition": {
        "string_equal": {
          "qcs:resource_tag": [
            "Department&Research and Development"
          ],
          "qcs:request_tag": [
            "Department&Research and Development"
          ]
        }
      }
```

Application of Boolean Condition Operators

Description

The sub-user must bind the token before the API key can be deleted.

Sample Code

The following example describes that the sub-users authorized by this policy need to bind the token before they can delete the API key.

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "cam:DeleteApiKey"
      ],
      "resource": [
        "*"
      ],
      "condition": {
        "bool_equal": {
          "qcs:BindToken": "true"
        }
      }
    }
  ]
}
```

Policy version control

Last updated：2023-08-31 18:29:06

Overview

When changes are made to your custom policy settings, the system will not overwrite the existing policy but will automatically create a new version. After saving, you can quickly revert to different policy versions by setting different versions as the default.

Permissions for setting the default policy version

The root account or sub accounts that have cam:ListPolicies, cam:GetPolicy, and cam:UpdatePolicy API permissions can configure default policy versions.
Root accounts can use the following policy syntax to give sub accounts permission to configure the default policy version:

```
    {
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "name/cam:ListPolicies",
        "name/cam:GetPolicy",
        "name/cam:UpdatePolicy"
      ],
      "resource": [
        "*"
  ]
}
  ]
}
```

Setting the default version for custom policies

You can set one of the versions of your custom policy as the default, or effective, version. Once set successfully, all sub-accounts associated with this custom policy will obtain the permissions set in the current default version.

1. Log in to the Cloud Access Management Console and navigate to the Policies management page.
2. On the policy management page, click the name of the custom policy you wish to configure to enter the policy details page.
3. On the policy details page, select **Policy Version**.
4. Locate the version you wish to set, check the box on the left, and click **Set as Default** to complete the operation of setting the default version for the custom policy.

Rolling back Changes by Using Different Versions

You can roll back your changes by setting the default version of your custom policy. For instance, consider the following scenario:
Create a custom policy that grants a sub-account read permissions for the cloud server ins-1. When created, the custom policy only has one version (marked as version 1), which is automatically set as the default version. This policy functions as expected.
When you update this custom policy, adding read permissions for the cloud server ins-2 based on the original policy, the system will create a new policy version (marked as version 2). After setting version 2 as the default, the sub-account reports a lack of cloud server management permissions. In this case, you can roll back the current policy to the functional policy version 1. By setting version 1 as the default, the sub-account can regain management of the original cloud server.
After identifying and updating the errors in policy version 2, the system will create another new version of the policy, marked as version 3. You can set version 3 as the default to grant the sub-account read permissions for two cloud servers, ins-1 and ins-2. At this point, you can delete the erroneous policy version 2.

Version Limitations

A custom policy can store up to 5 policy versions. When the number of policy versions for a custom policy reaches 5, you must delete one or more existing versions before you can successfully save your edits to the policy. You can choose from the following two methods to delete existing policy versions in the pop-up prompt:

- Delete the oldest non-default policy version.
- Select the policy versions you wish to delete (multiple selections allowed). You can click on the "▾" on the left to view the policy syntax of each version, to aid in your decision-making.

Note
When a particular version is deleted, the version identifiers of the remaining versions will not change. Therefore, the version identifiers may be discontinuous. For instance, if you delete policy versions 2 and 4, and then add two new versions, the remaining version identifiers might be versions 1, 3, 5, 6, and 7.

Scenarios where 'deny' in permission policy is ineffective

Last updated：2023-08-31 18:29:27

When a permission policy contains both "allow" and "deny" authorization statements, it is necessary to determine whether "deny" is effective based on the specific scenario.
This document elucidates the logic behind the ineffectiveness of 'deny' through three typical scenarios: operations involving the query of resource lists, COS permissions denying all users (anonymous users), and billing-related operations.

Operations pertaining to the querying of resource lists

Tencent Cloud's various service operations (actions) can be simply divided into four categories: addition, deletion, modification, and query. The query category can be further divided into querying individual resource details and querying a list of certain resources. In the following scenarios, 'deny' may not be effective. **It is recommended to avoid using 'deny' for these operations, as well as condition keys such as 'string_not_equal' and 'string_like'**.

Scenarios where 'deny' is ineffective include:

Scenario 1: If a sub-user is granted permission (allow) to access CVM instances a, b, and c, but denied (deny) access to instance d, and is also granted access to resources tagged with T, where instance d is tagged with T, the policy of "deny access to instance d" will not be effective.
For instance, when the following policy is authorized, the user can still view instance 'd' while viewing the CVM instance list.

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "*"
      ],
      "resource": "*",
      "condition": {
        "for_any_value:string_equal": {
          "qcs:resource_tag": [
            "key&T"  // Tag T
          ]
        }
      }
    },
    {
      "effect": "allow",
      "action": [
        "*"
      ],
      "resource": [
        "qcs::cvm:ap-guangzhou::instanceid/a",  // Instance a
        "qcs::cvm:ap-guangzhou::instanceid/b",  // Instance b
        "qcs::cvm:ap-guangzhou::instanceid/c"   // Instance c
      ]
    },
    {
      "effect": "deny",
      "action": [
        "*"
      ],
      "resource": [
        "qcs::cvm:ap-guangzhou::instanceid/d"   // Instance d
      ]
    }
    ]
}
```

Scenario 2: If a policy allows a sub-user to access resources tagged with T1 and denies access to resources tagged with T2, and resource 'a' is tagged with both T1 and T2, then the policy denying access to resource 'a' will not be effective.
For instance, even when the following policy is authorized, resource 'a' can still be viewed when inspecting the resource list.

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "*"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "key&T1"  // Tag T1
                    ]
                }
            }
        },
        {
            "effect": "deny",
            "action": [
                "*"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "key&T2"  // Tag T2
                    ]
                }
            }
        }
    ]
}
```

Scenario 3: When the permission policy includes a condition, policy condition keys that support precise matching, such as 'string_equal', 'ip_equal', 'ip_not_equal', etc., will be effective. Other types of condition keys (for example, 'string_not_equal', etc.) will not be effective.
For instance, even if the following policy is authorized, users may still be able to view resources associated with the tag 'T'.

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "*"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_not_equal": {
                    "qcs:resource_tag": [
                        "key&T"  // Tag T
                    ]
                }
```

```
      }
    }
  ]
}
```

Scenario 4: When both permissions to access all resources and denial of access to resources bound with specific tags are granted, the denial of access may not be effective, meaning that resources associated with that tag can still be viewed.
For instance, even if the following policy is authorized, users may still be able to view all resources under the root account when viewing the resource list.

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "*"
      ],
      "resource": "*"
    },
    {
      "effect": "deny",
      "action": [
        "*"
      ],
      "resource": "*",
      "condition": {
        "for_any_value:string_equal": {
          "qcs:resource_tag": [
            "key&T"  // Tag T
          ]
        }
      }
    }
  ]
}
```

COS permissions denying all users (anonymous users)

If 'deny' is configured for all users (anonymous users) in the COS Bucket ACL or Bucket Policy, but there is also a specific 'allow' for a certain user, the user allowed can still access the COS bucket.

Billing-related operations

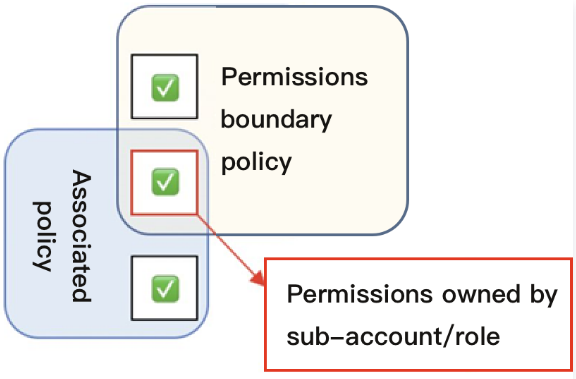
If a sub-user is associated with the AdministratorAccess or QCloudFinanceFullAccess policy, and is also associated with a policy that denies action finance:xx, this sub-user can still be authenticated for action finance:xx and will not be denied access.

Permissions Boundary

Last updated：2024-02-01 19:11:43

Concept

The permissions boundary is an advanced feature provided by Tencent Cloud for setting permissions boundaries for sub-accounts/roles. When you set a permissions boundary for a sub-account/role, the sub-account/role can only execute the intersection of the associated policies and its permissions boundary. The permissions boundary only limits the maximum permissions that a sub-account/role can have and cannot be used to set the permissions associated with the sub-account/role.
For a detailed evaluation logic, please refer to the following diagram:


Permissions boundary policy
Associated policy
Permissions owned by sub-account/role

Use Cases

You can use preset or custom policies to set permissions for sub-accounts/roles, which will define their maximum permissions. This document provides a typical case to help you understand how to use permissions boundaries to set the maximum permissions for a sub-account.
Assume that a company's Tencent Cloud resource administrator needs to set permissions for operations staff. The following requirements need to be met:

- The company has two Ops employees, each of whom has a sub-account: `test1` and `test2` , respectively.
- The employee with the `test1` sub-account only needs to manage all permissions for the MySQL cloud database under the main account.
- The employee with the sub-account `test2` only needs read access to manage the server with the instance ID `ins-1` under the main account.
- The company stipulates that all sub-accounts must operate within the company's network segment (10.217.182.3/24 or 111.21.33.72/24) for any operations related to the CVM and TencentDB for MySQL under the primary account.

Instructions

Setting permissions for sub-account `test1`

1. Log in to the company's admin account and navigate to the User List page.
2. On the user list page, find the sub-account `test1` and click the user's nickname to enter the user details page.
3. In the **Permissions - Policy** operation column, click **Associate Policy** and select the QcloudCDBFullAccess policy to set all permissions for the MySQL cloud database for the sub-account `test1` .
4. Click **Set Boundary** in the **Permissions - Permissions Boundary** operation column to enter the Set Permissions Boundary page.
5. On the Permissions Boundary page, click **Create Custom Policy** to navigate to the Create Custom Policy page.
6. On the Create Custom Policy page, set the policy name to **policygen-1**.
7. In **Visual Policy Generator**, add the following information:
   - Effect: Select **Allow**.
   - Service: Select **TencentDB for MySQL**.
   - Action: Select **All Actions**, and then click **OK**.
   - Resource: By default, it applies to all resources ("*").

- Condition: Select Source IP and supplement the IP values as **10.217.182.3/24, 111.21.33.72/24**.

8. Click **Create** to enter the Set Permissions Boundary page.
9. On the permissions boundary setting page, select the created custom policy in the policy list.
10. Click **Set Boundary** to complete the permission settings for the sub-account `test1`.

Setting permissions for sub-account `test2`

1. Log in to the company's administrator account and create a custom policy syntax named `policygen-2` following the policy syntax below. For the operation steps, please refer to Creating Custom Policies through Policy Syntax.

```
{
 "version": "2.0",
 "statement": [
    {
       "effect": "allow",
       "resource": [
          "qcs::cvm:gz::instance/ins-1"
       ],
       "action": [
          "name/cvm:*"
       ]
    }
 ]
}
```

2. On the User List page, locate the sub-account with the nickname `test2`, and click on the user nickname to enter the user details page.
3. In the **Permissions - Policy** operation bar, click **Associate Policy** and select the `policygen-2` policy to set the operation permissions for the `ins-1` cloud server for the `test2` sub-account.
4. Click **Set Boundary** in the **Permissions - Permissions Boundary** operation column to enter the Set Permissions Boundary page.
5. On the Permissions Boundary page, click **Create Custom Policy** to navigate to the Create Custom Policy page.
6. On the Create Custom Policy page, set the policy name to **policygen-3**.
7. In **Visual Policy Generator**, add the following information:
   - Effect: Select **Allow**.
   - Service: Select **Cloud Virtual Machine**.
   - Operation (Action): Select **Read operation**, then click **OK**.
   - Resource: By default, it applies to all resources ("*").
   - Condition: Select Source IP and supplement the IP values as **10.217.182.3/24, 111.21.33.72/24**.
8. Click **Create** to enter the Set Permissions Boundary page.
9. On the permissions boundary setting page, select `policygen-3` in the policy list.
10. Click **Set Boundary** to complete the permission settings for the sub-account `test2`.

> ⚠ **Note:**
> Permissions boundaries currently do not support resource list type interfaces.

Project and Tag

Last updated：2024-02-01 19:12:54

Project Synopsis

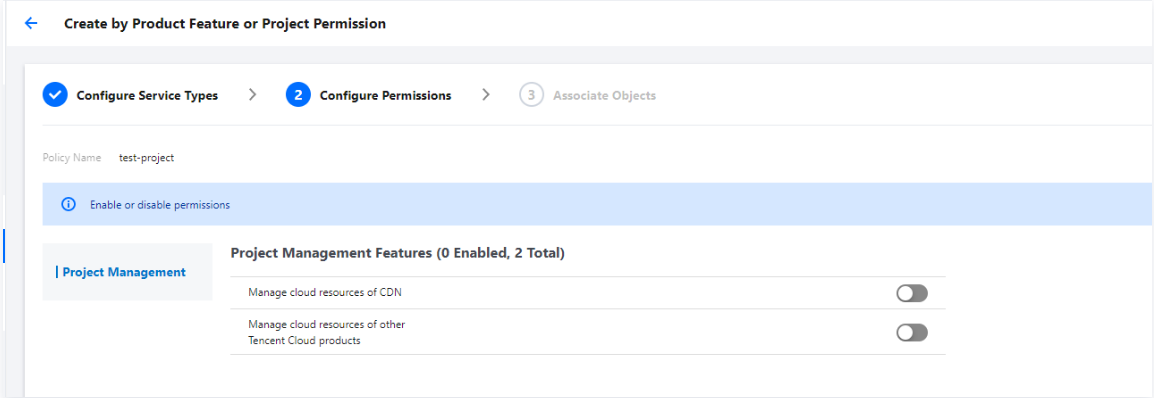
Project management is a centralized resource management system based on project dimensions. You can add cloud product resources that support the project feature to the project and generate project policies through **Create Custom Policy** > Create by Product Feature or Project Permission. You can associate project policies with project-related users or user groups to grant users operation permission to project resources.

> **Note**
> - Currently, project policies do not support creation through **Create by Policy Syntax**. Please generate project policies through Create by Product Feature or Project Permission. For instance, if you add a project ID to the resource (resource) field when creating a new policy syntax, an error will occur indicating that the resource field format is invalid.
> - The project policies generated through Create by Product Feature or Project Permission grant full access to all resources of all products added to the project, and do not support fine-grained permission management. For instance, they do not allow you to define read-only permission for the project on your own.
> - The project policies generated through Create by Product Feature or Project Permission cannot be edited. If you copy the policy syntax and create a new custom policy through **Create by Policy Syntax**, an error will occur indicating that the resource field format is invalid.

Create Project Policy

Tencent Cloud enables you to swiftly create project policies. Following the process outlined below, you can easily understand how to create policies for a specific project.

1. Log in to the Tencent Cloud console.
2. In the navigation bar at the top right, select the account dropdown list and click **Access Management** to enter the Cloud Access Management Console.
3. In the left sidebar, click **Policies** to navigate to the policy management page.
4. On the policy management page, click **Create Custom Policy**.
5. In the **Select the Creation Method** pop-up window, click **Create by Product Feature or Project Permission** to navigate to the creation page.
6. Enter the policy name, check **Project Management** in **Select Service Type**, and click **Next**.
7. Configure the project management feature according to actual needs.



Create by Product Feature or Project Permission

Configure Service Types > 2 Configure Permissions > 3 Associate Objects

Policy Name test-project

Enable or disable permissions

Project Management

Project Management Features (0 Enabled, 2 Total)

Manage cloud resources of CDN ○

Manage cloud resources of other Tencent Cloud products ○

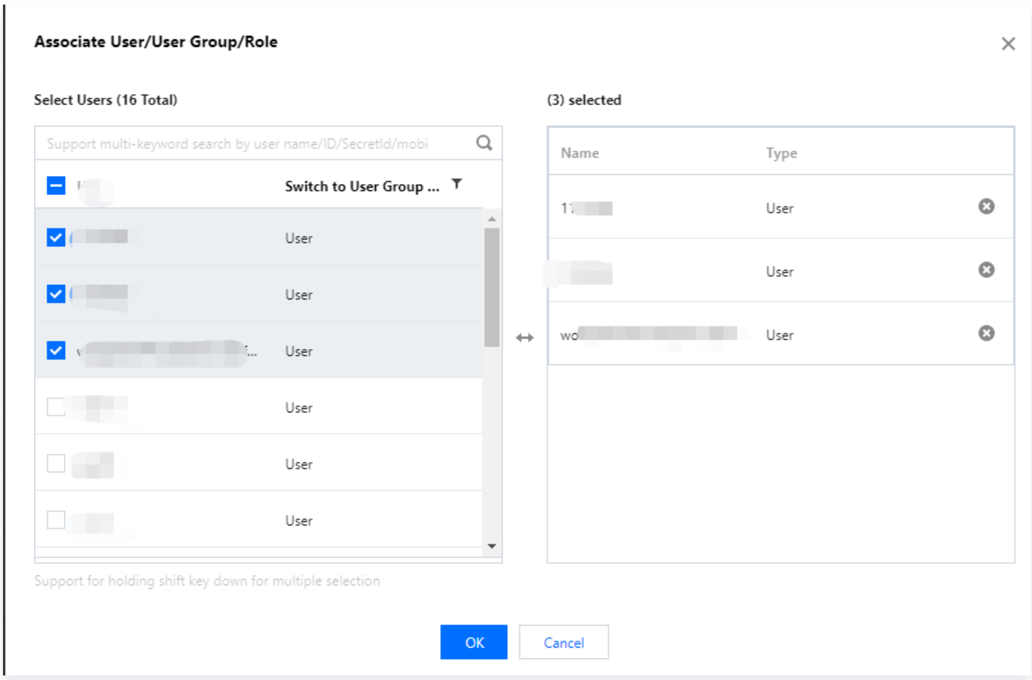
   - If you need to manage CDN-related project cloud resources, please set the ○ of **Manage CDN Business Project Cloud Resources** to ●.
   - If you need to manage project-related cloud resources of other products, please set the ○ of **Manage Cloud Resources in Other Business Projects** to ●.

8. Click **Next**.
9. In the "Project Management" list, click **Associate Object** and follow the interface prompts to limit the scope of the permission object.
   For example, if you intend to create a project management policy, you can click **Associate Object**, select **Select by Project**, and check the objects you need to manage in "Associate Object", then click **Confirm**.
10. Click **Finish**.

Grant Project Policies

Upon completion of creating a project policy, if you intend for users to have project permission, please associate this policy with the user or group.

1. Log in to the Tencent Cloud console.
2. In the navigation bar at the top right, select the account dropdown list and click Access Management to enter the Cloud Access Management Console.
3. In the left sidebar, click Policies to navigate to the policy management page.
4. In the search box, enter the name of the project management policy you created, press **Enter**, and view the policies that need to be associated with users or groups.
5. Click **Associate User/Group/Role** in the **Operation** column.
6. In the **Associate User/User Group/Role** window that appears, select the sub-account, user group, or role you wish to authorize, and click **OK** to grant the sub-account or user group project management permissions.



Associate User/User Group/Role

Select Users (16 Total)

Support multi-keyword search by user name/ID/SecretId/mobi

		Switch to User Group ...
☑	[redacted]	User
☑	[redacted]	User
☑	[redacted]	User
□	[redacted]	User
□	[redacted]	User
□	[redacted]	User

Support for holding shift key down for multiple selection

(3) selected

Name	Type
1[redacted]	User
[redacted]	User
wo[redacted]	User

> **Note**
> To revoke the project management permissions of a sub-account or user group, please disassociate it in **Associated Users/Groups** on the corresponding policy details page.

Tag-Based Project Resource Management

Currently, the traditional method of creating project policies grants full access to all resources of all products added to the project, and does not support fine-grained permission management. For instance, it does not allow you to define read-only permission for the project on your own. It is recommended to manage project resource permission using a tag-based approach. For more information about tags, see What Are Tags.

Advantages of Using Tags

A project is a one-dimensional marker and cannot meet complex management scenarios. Typical scenarios are as follows:

- A resource can only belong to one project and cannot be shared across multiple different projects.

- A resource can only be tagged with a single project, which does not meet the requirements for multi-dimensional tagging and classification.

Tags are two-dimensional markers, comprising tag keys and tag values, and are compatible with existing project capabilities. The project acts as a system tag, with the tag key being "project" and the tag value being the existing project.

- Tags can be used for fine-grained permission management of resources within a project.
- Billing can be organized according to tags.

Utilization of Tag Authorization

If you have created tags for resources and intend to grant a sub-account access to resources associated with one or more types of tags, you need to create a custom policy through Authorize by Tag. For more information, see Create Custom Policy by Tag Authorization.

Downloading Security Analysis Report

Last updated：2024-02-01 19:19:13

Scenario

You can download the User Credential Report to obtain the status of all Tencent Cloud sub-accounts and their user credentials, including console login passwords, access keys, and account security settings. This report can be used for compliance audits.

Instructions

1. Log in to the Cloud Access Management Console and navigate to the **Overview** page.
2. In the Security Analysis Report section, click **Download User Credential Report**. Follow the prompts to authenticate your identity. The system automatically generates the relevant report.
3. After the report is successfully downloaded, you can proceed to view it locally.

> **Note**
> A user credential report in CSV format is generated in the console every four hours. If you click **Download User Credential Report** within four hours after the last report is generated, you will get the same report rather than a new one.

Report Format

The User Credential Report is in CSV file format. You can open the CSV file with common spreadsheet software for analysis, or build an application to programmatically use the CSV file and perform custom analysis.
The CSV file contains the following information:

Parameter	Description	Value Description
Account ID	Account ID	Sub-account ID
Username	Username	Sub-account Username
UserType	User type	• Sub-user: A sub-user • Collaborator: Co-author • WeWork Sub-user: WeCom Sub-user • Message receiver: recipient of the message. For more details, see User Types.
CreationTime	Creation time	Example: 2019-08-16 9:25:56
PasswordEnabled	Is the console password enabled?	• TRUE: Enabled • FALSE: Not enabled. Console access has been disabled, and no login password has been set. • not_supported: N/A. WeWork-Sub-user (WeCom sub-user) logs in by scanning the WeCom QR code and does not have a login password; the message receiver (message recipient) is solely used for receiving messages and does not have a login password; the collaborator logs in using the primary account password and is not applicable to this item.
PasswordLastRotation	Last Password Modification Time	• FALSE: Console access has been disabled, and no login password has been set. • not_supported: N/A. WeWork-Sub-user (WeCom sub-user) logs in by scanning the WeCom QR code and does not have a login password; the message receiver (message recipient) is solely used for receiving messages and does not have a login password; the collaborator logs in using the primary account password and is not applicable to this item.
LoginConsoleActive	Support for console login	• TRUE: Supported • FALSE: Unsupported • not_supported: N/A. The message receiver is solely used for receiving messages

		and does not have a login password; the collaborator logs in using the primary account identity and is not applicable to this item.
LoginProtectionActive	Is login protection enabled?	• TRUE: Enabled • FALSE: Not enabled • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
OperationProtectionActive	Is operation protection enabled?	• TRUE: Enabled • FALSE: Not enabled • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
MFADeviceActive	Is MFA Enabled?	• TRUE: Enabled • FALSE: Not enabled • not_supported: N/A. The message receiver is only used for receiving messages and does not have a login password; the Sub-user has not bound any contact methods (mobile, WeChat).
Abnormal LoginsNumWithin30 Days	Unusual Logins in the Past 30 Days	• TRUE: Unusual logins detected. • FALSE: No unusual login activity detected.
AccessKey1SecretId	SecretId of Key 1	N/A: No key
AccessKey1MayBeAtRisk	Does Key 1 pose a risk of leakage?	• TRUE: Exposed to leakage risks • FALSE: No risk • N/A: No Key 1 • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey1CreationTime	Creation Time of Key 1	• N/A: No Key 1 • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey1Status	Key 1 Status	• Active: Enabled • Disable: Disabled • N/A: No Key 1 • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey1lastUsedDate	Last usage time of Key 1	• N/A: No Key 1 • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey1CreatedOver90Days	Has Key 1 been created for more than 90 days?	• N/A: No Key 1 • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey1CreatedOver30Days	Has Key 1 been created for more than 30 days?	• N/A: No Key 1 • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey2SecretId	SecretId of Key 2	N/A: No second key

AccessKey2MayBeAtRisk	Does Key 2 pose a risk of leakage?	• TRUE: Exposed to leakage risks • FALSE: No risk • N/A: No second key • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey2CreationTime	Creation Time of Key 2	• N/A: No second key • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey2Status	Key 2 Status	• Active: Enabled • Disable: Disabled • N/A: No second key • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey2lastUsedDate	Last usage time of Key 2	• N/A: No second key • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey2CreatedOver90Days	Has Key 2 been created for more than 90 days?	• N/A: No second key • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
AccessKey2CreatedOver30Days	Has Key 2 been created for more than 30 days?	• N/A: No second key • not_supported: N/A. The message receiver is solely for receiving messages and does not have a login password.
Last Console Login Time	Last Console Login Time	• N/A: No records available • not_supported: Console login not supported