Cloud Access Management

User Guide

Product Documentation

Tencent Cloud

©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

Trademark Notice

Tencent Cloud

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

Service Statement

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

Contents

©2013-2022 Tencent Cloud. All rights reserved.

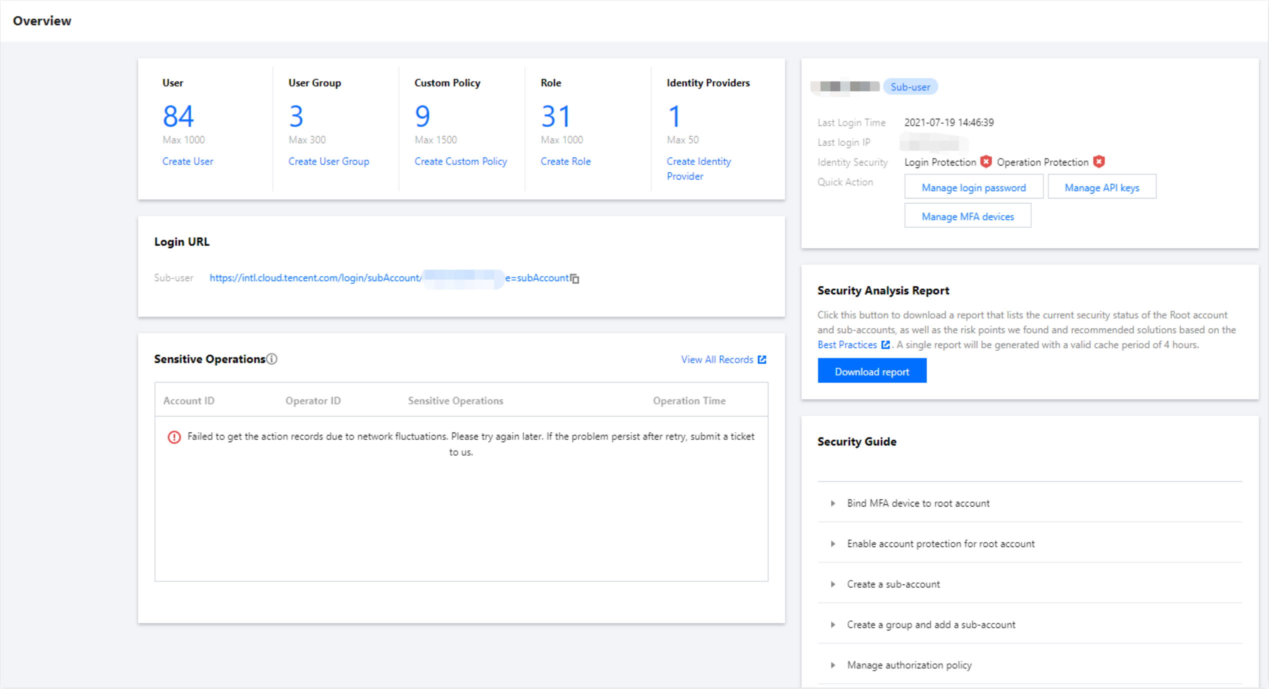
©2013-2022 Tencent Cloud. All rights reserved.

User Guide

Overview

Last updated：2024-01-23 17:29:58

The overview page in the CAM console has six modules: **CAM Resources**, **Login URL**, **Sensitive Operations**, **Last Login Info**, **Security Analysis Report**, and **Security Guide**.



Overview

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

Sub-user https://intl.cloud.tencent.com/login/subAccount/[redacted]e=subAccount

Sensitive Operations

View All Records

Account ID	Operator ID	Sensitive Operations	Operation Time
Failed to get the action records due to network fluctuations. Please try again later. If the problem persist after retry, submit a ticket to us.			

[redacted] Sub-user

Last Login Time 2021-07-19 14:46:39

Last login IP [redacted]

Identity Security Login Protection Operation Protection

Quick Action

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

- 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

Overview Page Permission

Users **associated with the `QcloudCamSummaryAccess` policy** can view the information of all modules when they log in to the console.

Users **not associated with the `QcloudCamSummaryAccess` policy** will only see the **Login URL** and **Last Login Info** modules.

The root account and the admin user (AdministratorAccess) are associated with this policy by default.

Sub-accounts can contact the root account (on the **User List** > **User Details** page) to check whether they have the permission of the `QcloudCamSummaryAccess` policy.

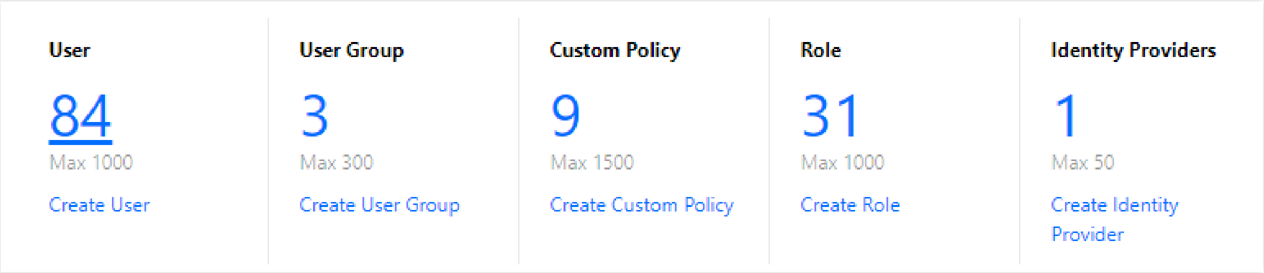
The root account can associate the `QcloudCamSummaryAccess` policy with sub-accounts as needed to allow them to view the information on the overview page in the console. For more information on the authorization method, please see Authorization Management.

©2013-2022 Tencent Cloud. All rights reserved.

Overview Page Modules

CAM resources

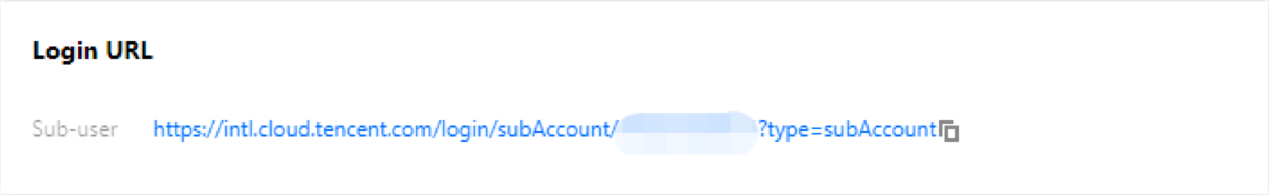
The CAM resources module displays the numbers of users, user groups, custom policies, roles, and identity providers created under the current root account. You can create more resources by clicking the button below each resource quantity.



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 URL for the sub-user. Both the root account and the sub-account can copy the URL by clicking the "Copy" icon on the right of the URL.



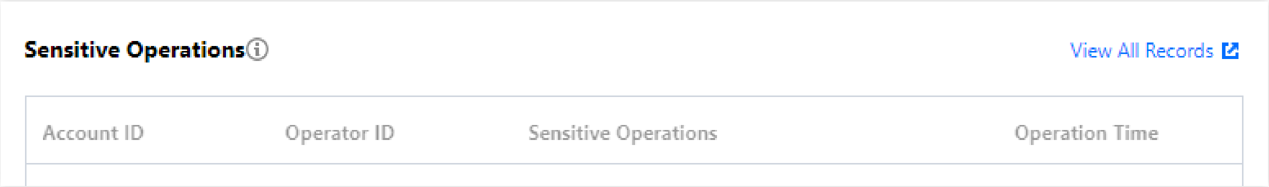
Login URL

Sub-user   https://intl.cloud.tencent.com/login/subAccount/[redacted]?type=subAccount

Sub-user login URL: applies to sub-users.

Sensitive operations

The sensitive operations module displays the overview information of all sensitive operations under the current root account in the last 3 days (up to 50 entries). The displayed information includes account ID, operator ID, sensitive operation details, and operation time. You can also click **View All Records** to enter the Cloud Audit console to view more detailed sensitive operation records.

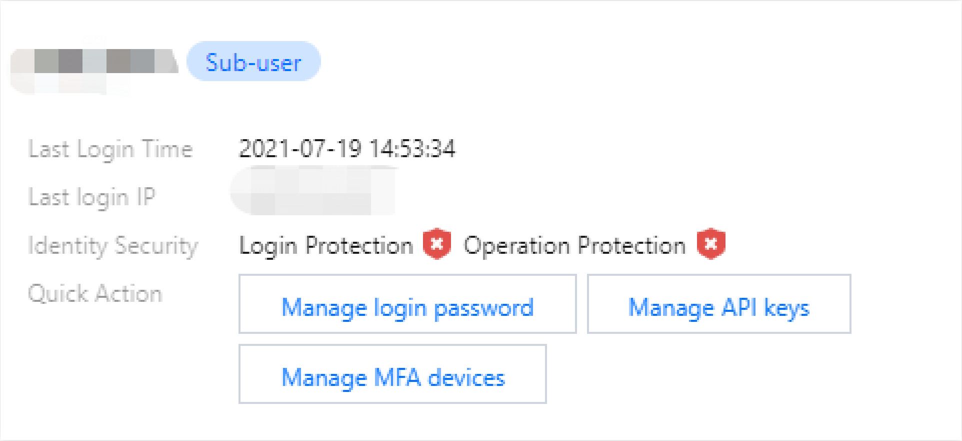


Sensitive Operations

Account ID	Operator ID	Sensitive Operations	Operation Time

Last login info

The last login info module displays the last login time, last login IP, identity security status, and shortcuts to manage API keys and manage MFA settings.

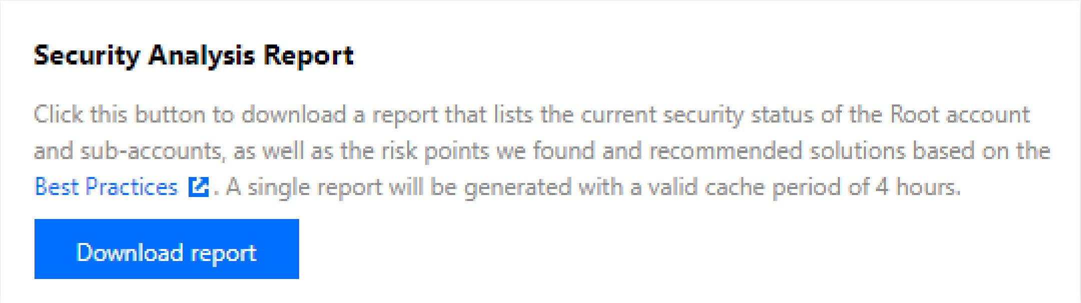


[redacted] Sub-user

Last Login Time	2021-07-19 14:53:34
Last login IP	[redacted]
Identity Security	Login Protection ✗ Operation Protection ✗
Quick Action	Manage login password Manage API keys Manage MFA devices

Security analysis report

The security analysis report module provides a **Download report** button. Click this button to get the security status of the current root account and sub-account, security risks discovered based on best practices, and recommended solutions. Each generated report will be cached for 4 hours.



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:

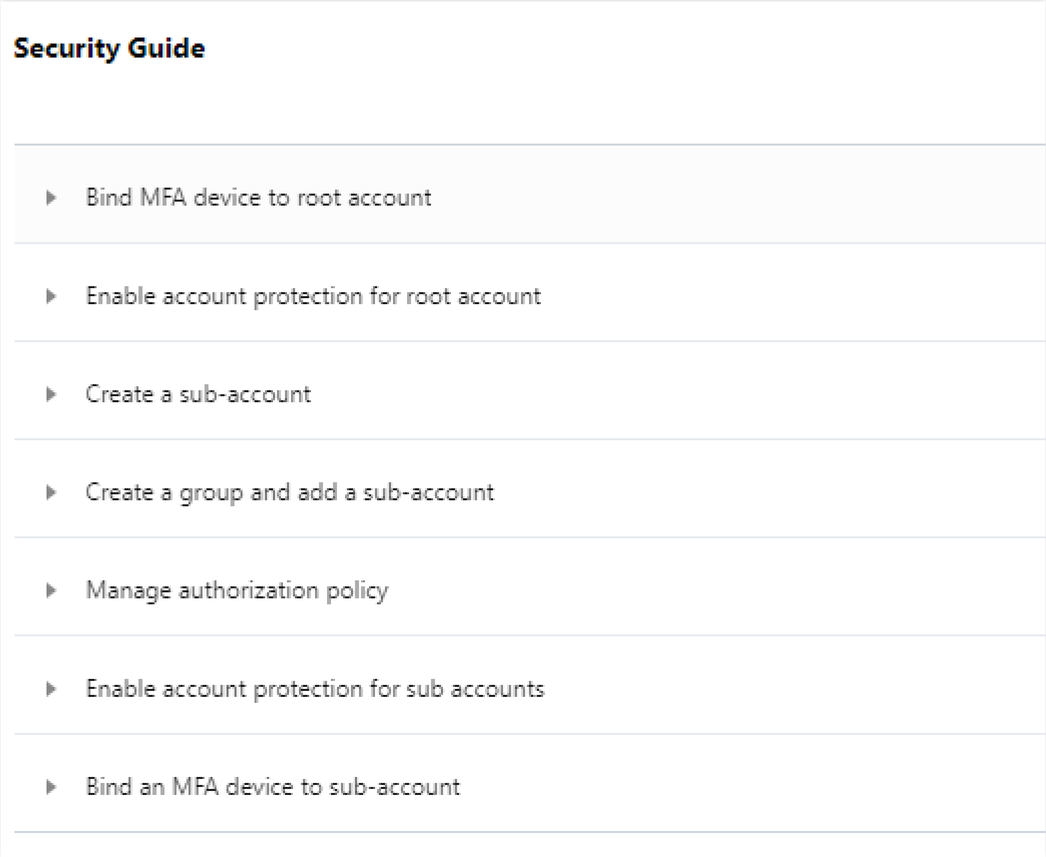
For the security of your accounts and assets in Tencent Cloud, we strongly recommend you complete all the configurations in the security guide.

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.

Operation permission: the **Bind MFA device to root account** and **Enable account protection for root account** features can be used only by the root account, while the other five features can be used by all authorized users.

Feature status: each feature has two status: **Not Completed** and **Completed**. The root account user can view the status of each feature. Sub-accounts cannot view feature status.

Feature link: sub-accounts with permissions can view feature descriptions and links by clicking the triangle icon to the left of each guide item. The following figure shows the security guide module the root account sees.



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：2024-01-23 17:29:58

Introduction

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

Prerequisites

You have signed up for a Tencent Cloud account, which is the root account. For more information, please see Sign up for a Tencent Cloud Account.

Directions

Root account does not require authorization

By default, a root account owns all the Tencent Cloud resources under it and can access any resources with no authorization required. Therefore, we do not recommend using the root account to access resources. You should create sub-accounts and grant them permissions based on the principle of least privilege and then use such sub-accounts with limited permissions to access your Tencent Cloud resources. For more suggestions on using account permissions, please see Best Practices.

Root account message channels

The recovery mobile number and email address set when you signed up for your Tencent Cloud root account will also be used as the default message channels. Please note that modifications made in Account Center are not synced to the CAM Console. If you wish to modify these message channels, please see Root Account Message Subscriptions.

Note:

In order to avoid potential losses caused by missed messages, please go to the CAM Console to check whether the contact mobile number or email address used for message subscription is correct.

Relevant Documents

©2013-2022 Tencent Cloud. All rights reserved.

For more information on how to change the recovery mobile number or email address for a root account, please see FAQs About Email Address and Mobile Number.

For more information on how to create a sub-user, please see Creating a Custom Sub-user.

For more information on how to configure sub-account permissions, please see Authorization Management.

©2013-2022 Tencent Cloud. All rights reserved.

Root Account Message Subscription

Last updated：2024-01-23 17:29:58

Introduction

This document describes how to verify and modify message channels and set message subscriptions for the root account. The root account must first verify the message channel before it can receive messages. The root account will receive messages after it has set up message subscriptions and have verified the message channel.

Prerequisites

Log in to the CAM Console and click User List.

Directions

Verifying message channels

1. Locate the root account from the user list.
2. Click **Username** to enter the user details page.
3. Click **Send Verification Link** in the user information section. If you do not see this, it means that the message notification channel has already been verified, and the following operations are not required.

Mobile: the system will send a verification message to the mobile number attached to the root account. Click on the link in the message to verify this channel.

Email: the system will send a verification message to the email address attached to the root account. Click on the link in the message to verify this channel.

Modifying message channels

1. Locate the root account from the user list.
2. Click **Username** to enter the user details page.
3. On the user details page, click **Modify** in the top-right corner.
4. Change the mobile number and email address as needed on the pop-up page.
5. You need to verify the message channel after making the change. For detailed directions, please see Verifying message channels.

Setting message subscriptions

1. Locate the root account from the user list.
2. Click **More** > **Subscribe to Messages** in the **Operation** column on the right.
3. On the "Subscribe to Messages" window that pops up, check to select the messages you want to receive (click "►" to expand the option list).
4. Click **Confirm**.

Relevant Documents

For more information on how to set up message subscriptions for a collaborator, please see Collaborator Message Subscriptions.

For more information on how to set up message subscriptions for a sub-user, please see Sub-User Message Subscriptions.

For more information on how to set up message subscriptions for a message recipient, please see Message Recipient Message Subscriptions.

©2013-2022 Tencent Cloud. All rights reserved.

Sub-Users

Creating Sub-User

Last updated：2024-01-23 17:35:43

Overview

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 CAM console and bind the sub-user to a permission policy.

Note:

Both sub-users and collaborators are sub-accounts. For related definitions and permission descriptions, see User Types.

Creation Method	Applicable Scenario	Description
Quick creation	Creating admin users	They have the `AdministratorAccess` permission by default, which can be modified
Custom creation	Creating general sub-users and message recipients	They can be bound to permission policies as needed

Prerequisites

A sub-account with admin permissions or a sub-account with `QcloudCamFullAccess` has been created.

Directions

Creating in the 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

©2013-2022 Tencent Cloud. All rights reserved.

Custom creation

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

Note:

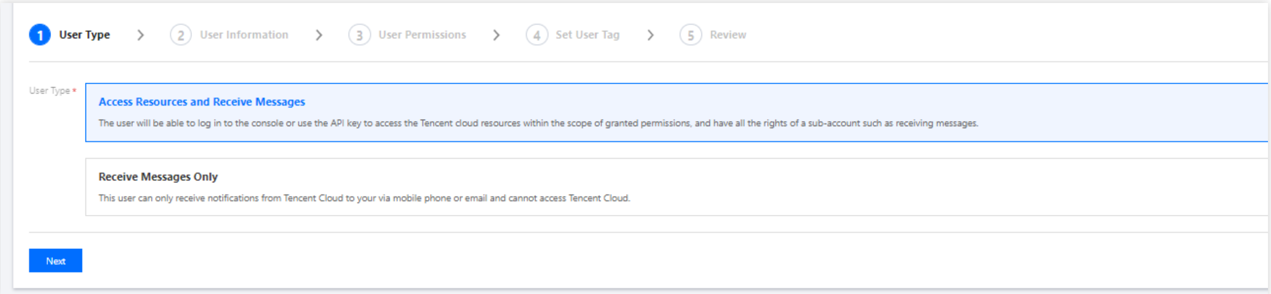
You can click **Create User** to create up to ten users at a time.

4. For **Password resetting required**, select whether the sub-user needs to reset the password upon next login as needed.
5. Click **Create User**. You will be redirected to the page prompting that the user is successfully created.
6. On the page prompting that the user is successfully created, you can get the sub-user information in the following two methods:

Click **Send**, enter the email address, and the system will send the complete sub-user information to the specified email address.

Click **Copy** and paste the information to a local file for storage.

1. Log in to the CAM console and select **Users** > **User List** on the left sidebar.
2. On the **User List** page, click **Create User** to enter the **Create User** page.
3. On the **Create User** page, click **Custom Creation** to enter the **User Type** page.
4. On the **User Type** page, select **Access Resources and Receive Messages** or **Receive Messages Only** and click **Next** to enter the user information.



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. Enter and confirm the information as prompted and click **Complete**.

If you select **Access Resources and Receive Messages**, you will be redirected to the page prompting that the user is successfully created.

If you select **Receive Messages Only**, you will be redirected to the **User List** page.

Creating through APIs

You can create a sub-user and configure permissions for them by calling the `AddUser` API with an access key. For more information, see AddUser.

Relevant Documents

For more information on how to manage and authorize sub-users through user group, see Managing User Groups and Associating/Unassociating Policy with/from User Group.

For more information on how to associate/dissociate a sub-user to/from policies, see Setting Sub-user Permissions.

For more information on how to log in as a sub-user, see Logging in as a Sub-User.

For more information on how to reset a sub-user password, see Resetting Login Passwords for Sub-users.

For more information on how to subscribe to messages for a sub-user, see Sub-user Message Subscriptions.

©2013-2022 Tencent Cloud. All rights reserved.

Setting Sub-User Permissions

Last updated：2024-01-23 17:35:43

Overview

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

Directions

Associating a policy with a sub-user

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 CAM Console and enter User List.
2. Locate the sub-user you want to grant permission to.
3. Click **Grant Permission** in the "Operation" column on the right.
4. In the "Associate Policies" window that pops up, select one or more policies to be associated.
5. Click **OK** to associate the policies with the sub-user.

Association via group

You can add a user to a user group to automatically grant the user permissions included in the policies that are associated with the user group. The policy types obtained by the user in this method depend on the policies associated with the user group. If you need to disassociate the user from a policy that is associated with the user group, you must remove the user from the user group.

1. Log in to the CAM Console and enter User List.
2. Locate the sub-user you want to grant permission to.
3. Click **More** > **Add to Group** in the "Operation" column on the right.
4. Select one or more user groups you want to add the sub-user to.
5. Click **OK** to add the sub-user to the user groups and associate the sub-user with the group-associated policies.

Disassociating a sub-user from a policy

Direct disassociation

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

1. Log in to the CAM Console and enter User List.

©2013-2022 Tencent Cloud. All rights reserved.

2. Locate the sub-user you want to remove permission from.
3. Click the name of the sub-user to enter the user details page.
4. Go to **Permissions** and locate the policy.
5. Click **Disassociate** in the operation column on the right.
6. Click **OK** to complete the disassociation. This user will no longer have the permissions described in the policy.

Removing a user from a group

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

1. Log in to the CAM Console and enter User List.
2. Locate the sub-user you want to remove permission from.
3. Click the name of the sub-user to enter the user details page.
4. Go to **Group** and locate the policy to be disassociated from.
5. Click **Remove from Group** > **Confirm** in the "Operation" column on the right to remove the sub-user from the user group.
6. After the removal, the user will no longer have the permissions associated with the user group.

Sub-User Security Credentials

Logging in as a Sub-User

Last updated：2024-01-23 17:35:43

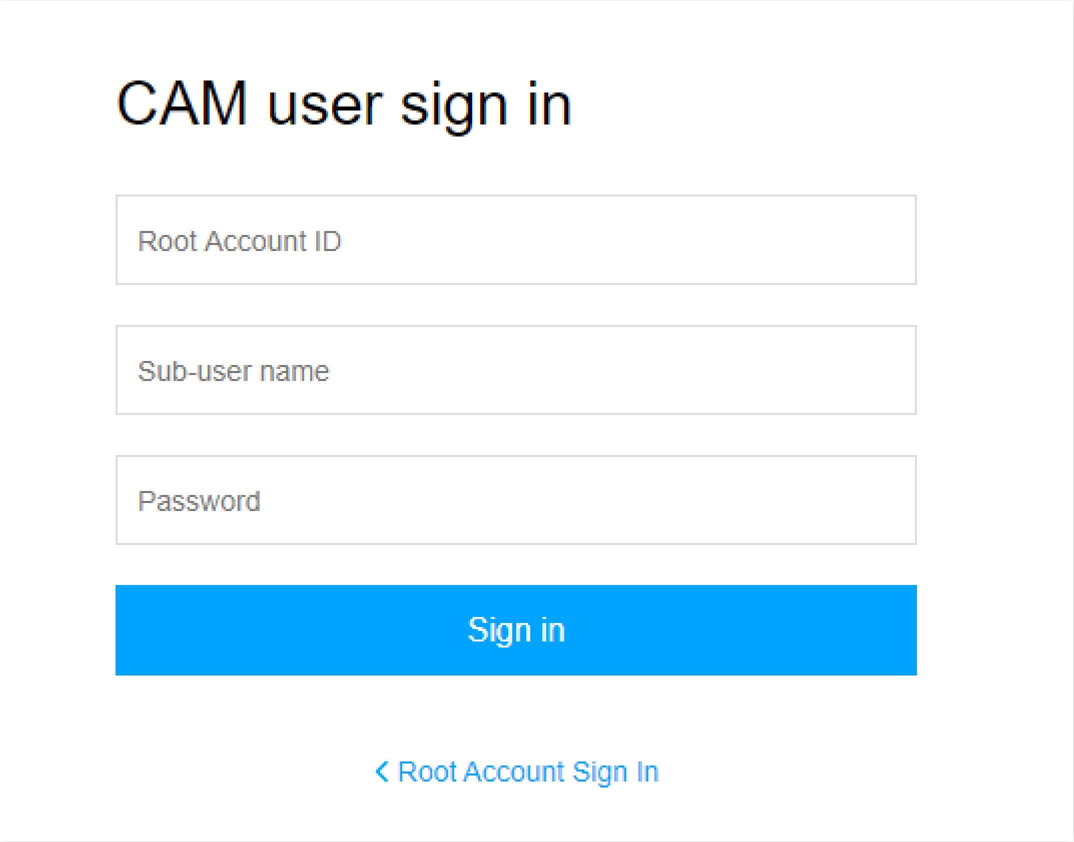
Introduction

This document describes how to log in as a sub-user. After logging in, sub-users can manage resources belonging to the root account within the scope of permissions granted.

Directions

Logging in as a sub-user

1. Go to Sign in as a CAM user.
2. Enter the root account ID, sub-user name, and login password, as shown in the following figure:



CAM user sign in

Note：

The root account ID (e.g., 100001234567) is the ID of the root account to which the sub-user belongs. This is the unique identifier of the account in Tencent Cloud and can be viewed in Account Information. Contact the root account to get the ID.

3. Click **Sign in** to log in as a sub-user.

Resetting Login Passwords for Sub-Users

Last updated：2024-01-23 17:35:43

Overview

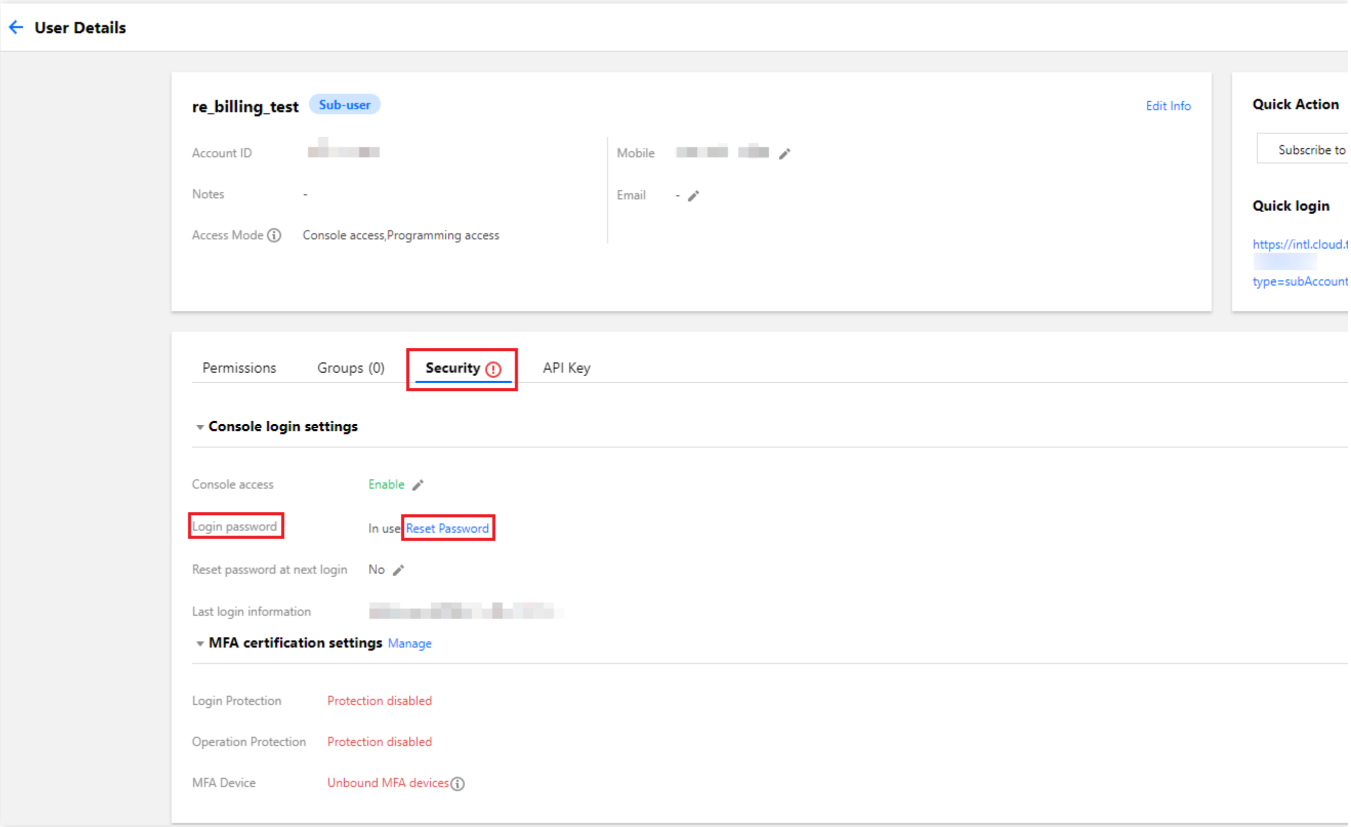
This document describes how to change the password for a sub-user. After the modification, the sub-user can use the new password to log in and manage resources under the root account.

Directions

Note:

These directions only apply to created custom sub-users.

1. In User List, locate the sub-user whose password needs to be changed and click the **username** to enter the user details page.
2. Go to **Security** > **Console login settings** > **Login password** and click **Reset Password**, as shown below:



User Details

re_billing_test Sub-user

Edit Info

Account ID [redacted]

Notes -

Access Mode Console access,Programming access

Mobile [redacted]

Email -

Quick Action

Subscribe to

Quick login

https://intl.cloud.t [redacted] type=subAccount

Permissions Groups (0) Security API Key

Console login settings

Console access Enable

Login password In use Reset Password

Reset password at next login No

Last login information [redacted]

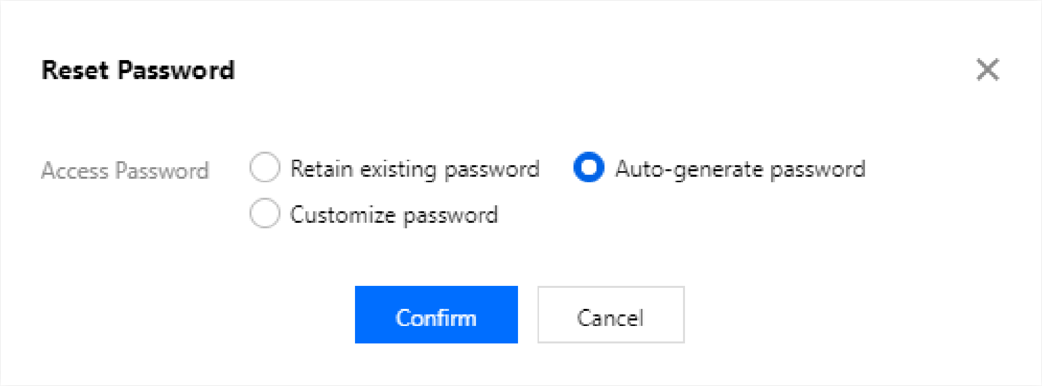
MFA certification settings Manage

Login Protection Protection disabled

Operation Protection Protection disabled

MFA Device Unbound MFA devices

3. In the **Console Access** window that pops up, set the password for the current user 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 the following two ways:

If you select **Auto-generate password** in **Access Password**, the system will automatically generate a console login password. You can copy and save it. If needed, you can also click **Download .csv** to save the password.

If you select **Customize Password** in **Access Password**, enter the password you want to set as the sub-user's console login password.

If you want the current user to reset their own password, you can select **Enforce Password Reset**. The sub-user will be required to reset their console login password the next time they log in.

Related documents

For more information on how to create custom sub-users, please see Creating a Custom Sub-user.

For more information on how to change the login password for collaborators, please see Modifying Account Password.

Setting Security Protection for Sub-Users

Last updated：2024-01-23 17:35:43

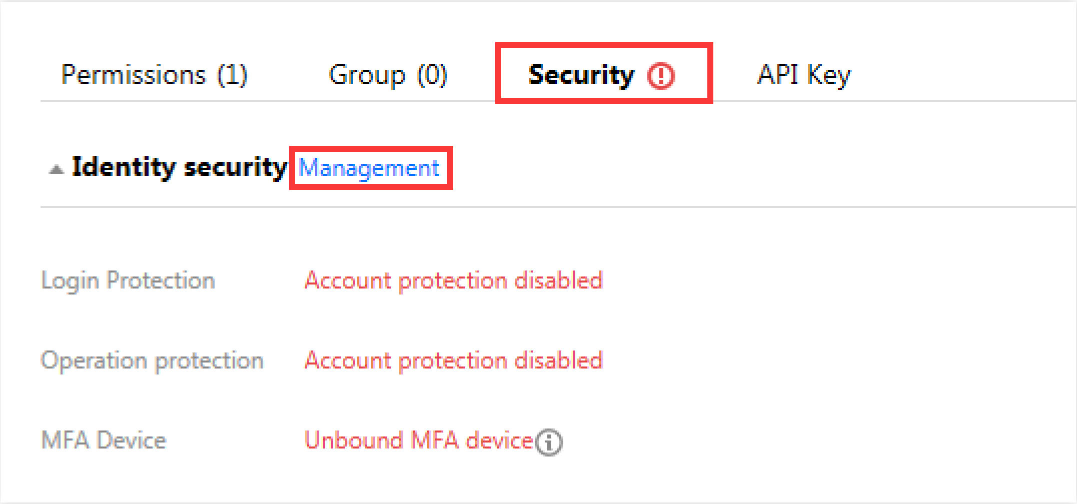
Operation Scenarios

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

Directions

Enabling security protection for sub-user

1. Log in to the CAM Console and select **Users** > **User List** on the left sidebar.
2. In the user LIst management page, locate the sub-user you want to configure security protection for.
3. Click the **username** to go to the user details page.
4. On the user details page, click **Security** to go to the security management section.
5. On the security management page, click **Manage** next to "Identity Security" as shown below:



Login Protection Account protection disabled

Operation protection Account protection disabled

MFA Device Unbound MFA device

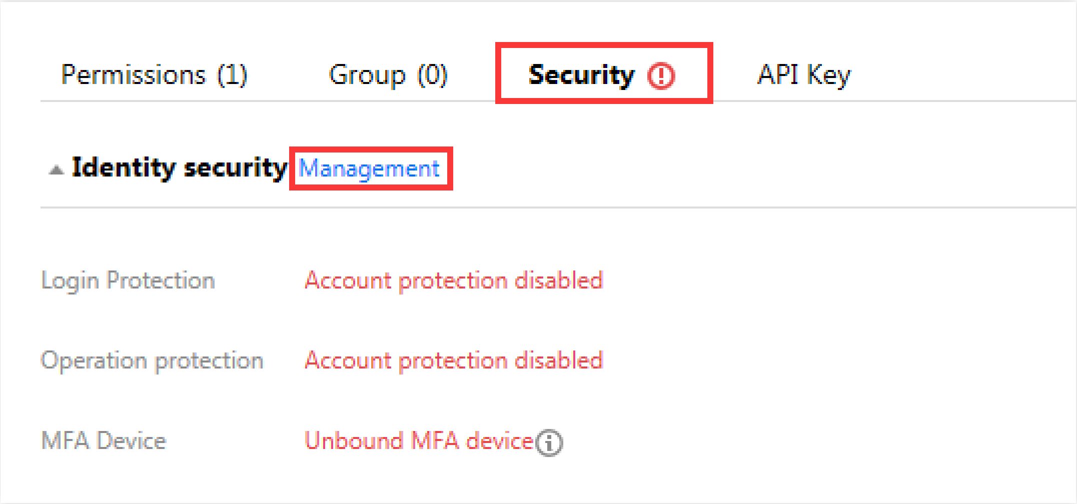
6. In the identity security window that pops up, select the protection type you want to enable for the sub-user.
7. Click **OK** to complete enabling security protection for the sub-user.

Note:

If virtual MFA device verification is enabled, the sub-user will need to bind the MFA device the next time they log in.

Disabling security protection for sub-user

1. Log in to the CAM Console and select **Users** > **User List** on the left sidebar.
2. In the user list management page, locate the sub-user you want to configure security protection for.
3. Click the **username** to go to the user details page.
4. On the user details page, click **Security** to go to the security management section.
5. On the security management page, click **Manage** 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 sub-user.
7. Click **OK** to complete disabling security protection for the sub-user.

Sub-User Message Subscriptions

Last updated：2024-01-23 17:35:43

Overview

This document describes how to verify message channels and set message subscriptions for a sub-user. The sub-user must first verify the message channels before they can receive messages. They will then receive subscribed messages through the verified message channels.

Directions

Verifying message channel

1. Log in to the CAM Console and enter User List.
2. Locate the sub-user to set the message subscription for.
3. Click the **username** to enter the user details page.
4. On the user details page, click **Send verification link** next to a user message channel.

Mobile: the system will send a verification message to the mobile number set for the sub-user. Click on the link in the message to verify this channel.

Email: the system will send a verification message to the email address set for the sub-user. Click on the link in the message to verify this channel.

Setting message subscription

1. Log in to the CAM Console and enter User List.
2. Locate the sub-user to set the message subscription for.
3. Click **More** > **Subscribe to Message** in the "Operation" column 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 **Confirm** to complete setting the message subscription.

Querying Sub-User Information

Last updated：2024-01-23 17:35:43

Overview

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.

Prerequisites

Log in to the CAM Console and enter the User List management page.

Directions

Expanding to view sub-user information

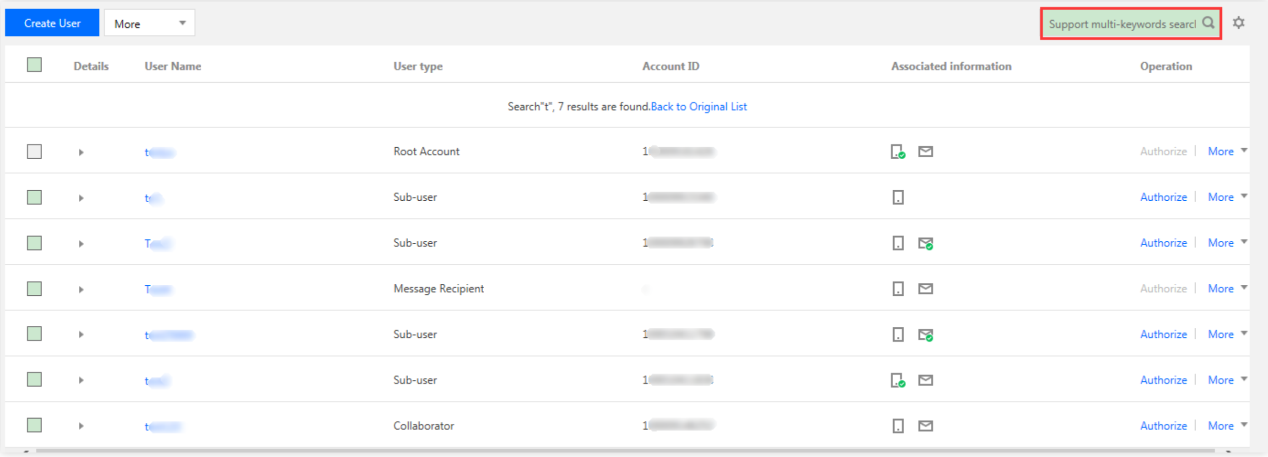
You can expand to view sub-user information, which includes user groups, message subscriptions, login protection, operation protection, MFA device status, and console access status.

1. On the user list management page, locate the sub-user that you want to view.
2. Click the details column icon (▶) on the left.
3. View the information of the sub-user in the expanded section.

Using search box to search for sub-user

You can search for sub-users by using keywords such as username, account ID, `SecretId` , mobile phone, email, or notes.

1. On the user list management page, locate the search box in the top-right corner.
2. In the search box, enter the keyword and click the search icon on the right to search for sub-users as shown below:



Create User | More ▾ | Support multi-keywords searcl

☐	Details	User Name	User type	Account ID	Associated information	Operation
Search"t", 7 results are found.Back to Original List						
☐	▸	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 ▾

Deleting Sub-Users

Last updated：2024-01-23 17:35:43

Introduction

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

Prerequisites

Log in to the CAM Console and enter the User List management page.

Directions

Deleting one single sub-user

1. In the User List management page, locate the sub-user that you want to delete.
2. Click **More** > **Delete** in the "Operation" column on the right.
3. In the pop-up window, confirm that the API key under the current sub-user has been disabled and deleted. For more information, please see Access Key.
4. Click **Delete** to delete the sub-user.

Deleting 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 **More** > **Delete** in the top-left corner.
3. In the pop-up window, confirm that the API keys under the selected sub-users have been disabled and deleted. For more information, please see Access Key.
4. Click **Delete** to delete the selected sub-users.

©2013-2022 Tencent Cloud. All rights reserved.

Disabling Sub-User

Last updated：2024-07-17 10:17:15

Overview

This document describes how to disable a single sub-user. Once disabled, the sub-user cannot log in to the console or programmatically access the resources within this account, and will no longer receive messages. Additionally, disabling a sub-user will simultaneously disable the following 3 permissions of the sub-user, namely logging in to the console, using all current API keys, and receiving subscription and system messages. If you want to enable this sub-user again, see Enabling Disabled Sub-User.

Prerequisites

Log in to the CAM console and enter the User List page.

Directions

1. On the **User List** page, locate the sub-user that you want to disable.
2. Click **More** > **Disable** in the Operation column on the right.
3. In the pop-up **Disable User** window, click **Disable** to complete disabling the sub-user.

Enabling Disabled Sub-User

Last updated：2024-07-17 10:17:36

Overview

This document describes how to enable a disabled sub-user. After the 3 disabled permissions are enabled successively, the sub-user can log in to the console or programmatically access the resources within this account, and receive messages again. If you want to disable this sub-user again, see Disabling Sub-User.

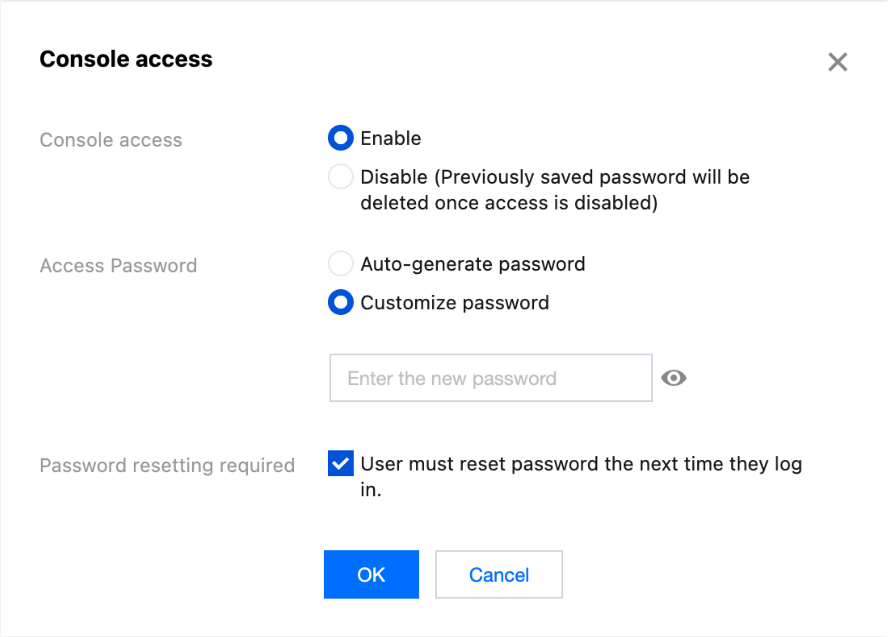
Prerequisites

Log in to the CAM console and enter the User List page.

Directions

Enabling the Sub-User's Console Access Permission

1. On the **User List** page, locate the sub-user that you want to enable.
2. Click the sub-user's **username** to enter the **User Details** page.
3. On the **User Details** page, click **Security** > **Console Login Settings** > **Console Access**, and then click on ✎ on the right.
4. In the pop-up **Console Access** window, check **Enable** and select the relevant information as needed, as shown in the figure below:



Console access

Console access: ● Enable ○ Disable (Previously saved password will be deleted once access is disabled)

Access Password: ○ Auto-generate password ● Customize password

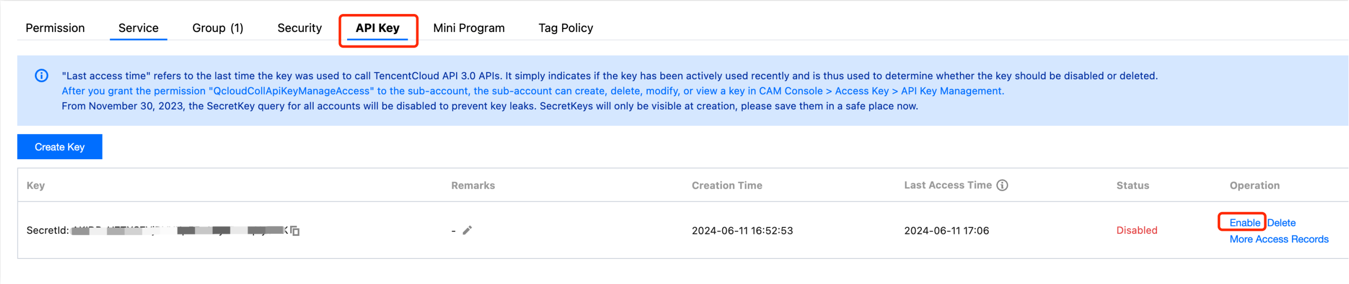
Enter the new password

Password resetting required: ☑ User must reset password the next time they log in.

5. Click **OK**.

Enabling the Sub-User's Access Key Permission

1. On the **User List** page, locate the sub-user that you want to enable.
2. Click the sub-user's **username** to enter the **User Details** page.
3. On the **User Details** page, click **API Key** and then click **Enable**, as shown in the figure below:

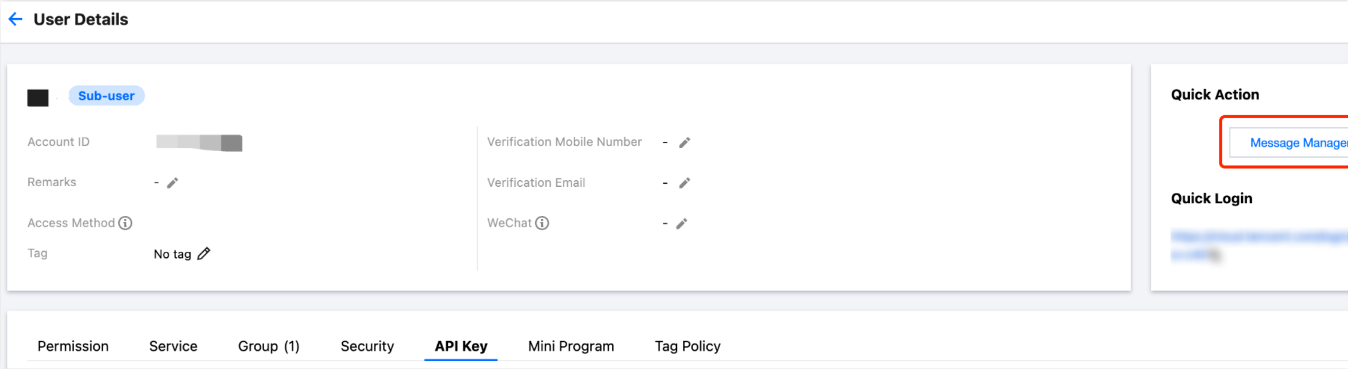


"Last access time" refers to the last time the key was used to call TencentCloud API 3.0 APIs. It simply indicates if the key has been actively used recently and is thus used to determine whether the key should be disabled or deleted.
After you grant the permission "QcloudCollApiKeyManageAccess" to the sub-account, the sub-account can create, delete, modify, or view a key in CAM Console > Access Key > API Key Management.
From November 30, 2023, the SecretKey query for all accounts will be disabled to prevent key leaks. SecretKeys will only be visible at creation, please save them in a safe place now.

Key	Remarks	Creation Time	Last Access Time	Status	Operation
SecretId: [redacted]	-	2024-06-11 16:52:53	2024-06-11 17:06	Disabled	Enable Delete More Access Records

Enabling the Sub-User's Message Receiving Permission

1. On the **User List** page, locate the sub-user that you want to enable.
2. Click the sub-user's **username** to enter the **User Details** page.
3. On the **User Details** page, click **Quick Action > Message Management**.



User Details

[redacted] Sub-user

Account ID [redacted]

Remarks -

Access Method

Tag No tag

Verification Mobile Number -

Verification Email -

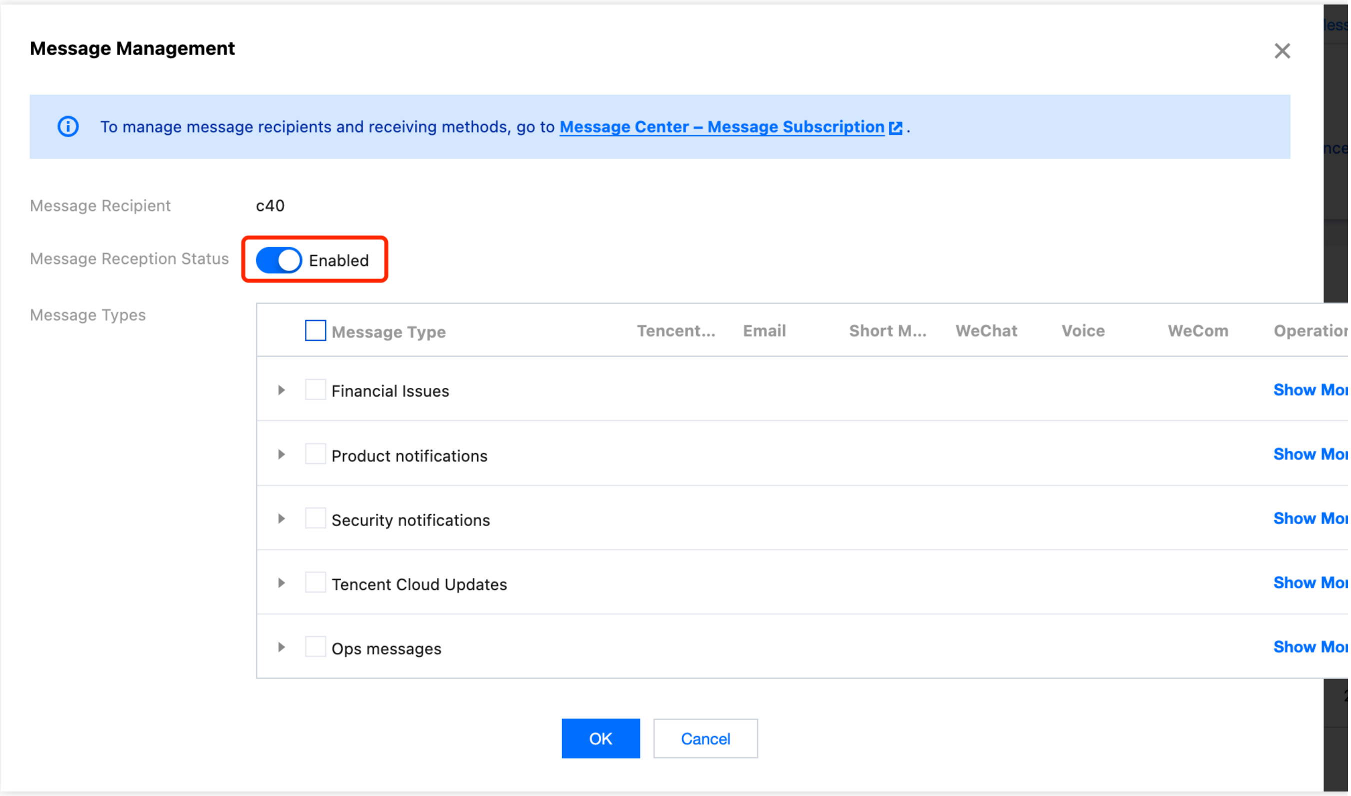
WeChat -

Quick Action

Quick Login

[redacted]

4. In the pop-up **Message Management** window, click on ◯ to the right of **Message Reception Status**. After setting the status to **Enabled**, you can select the subscription message type as needed, and then click **OK**.



Message Management

To manage message recipients and receiving methods, go to Message Center – Message Subscription .

Message Recipient c40

Message Reception Status Enabled

Message Types

□ Message Type	Tencent...	Email	Short M...	WeChat	Voice	WeCom	Operatior
□ Financial Issues							Show Moi
□ Product notifications							Show Moi
□ Security notifications							Show Moi
□ Tencent Cloud Updates							Show Moi
□ Ops messages							Show Moi

Collaborators

Creating Collaborator

Last updated：2024-01-23 17:31:58

Overview

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 CAM console and bind the collaborator to a permission policy.

Note:

Both collaborators and sub-users are sub-accounts. For related definitions and permission descriptions, please see User Types.

Prerequisites

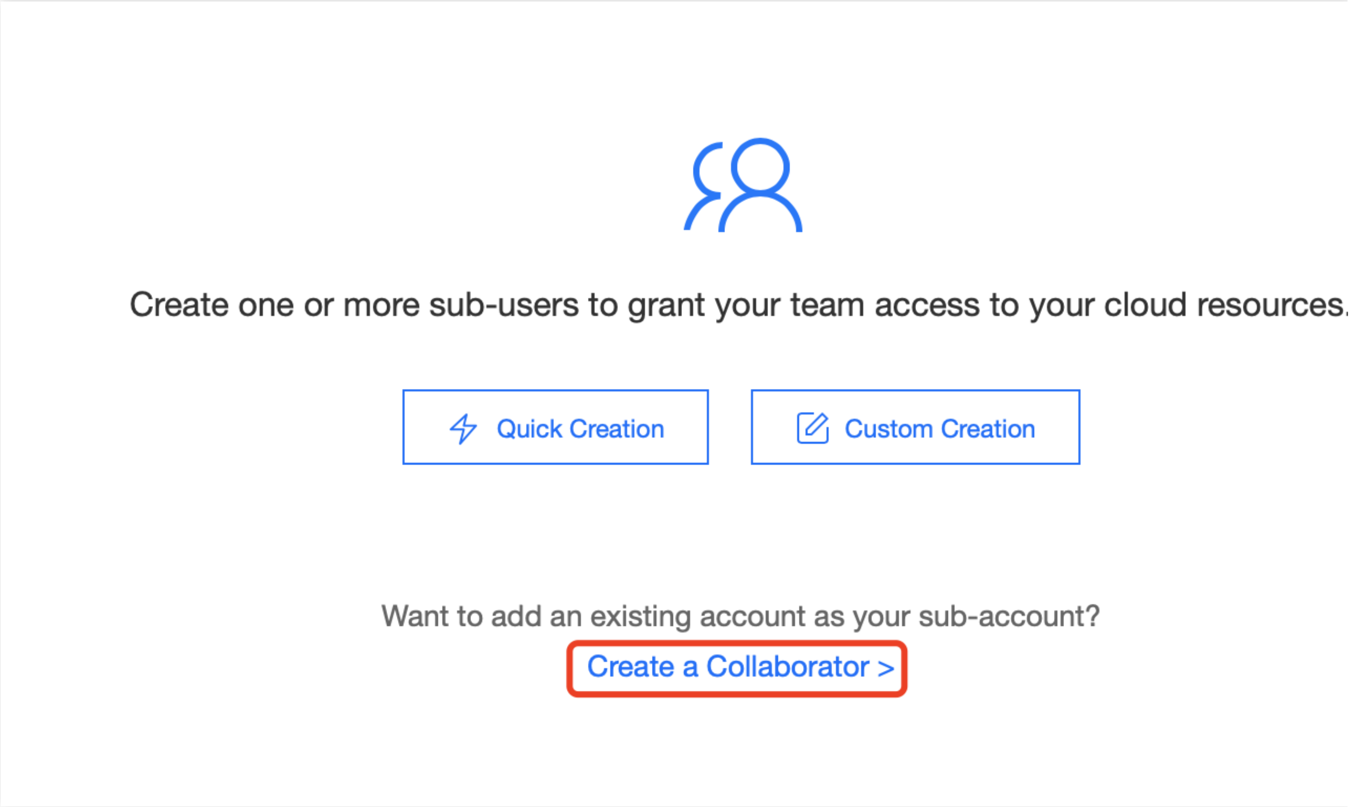
An admin user has been created.

There is an existing Tencent Cloud account that can be set as a collaborator (if not, sign up for one first).

Directions

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

©2013-2022 Tencent Cloud. All rights reserved.



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?

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

Note:

Collaborators are allowed to log in to the Tencent Cloud console by default. Cancellation of this permission is not supported currently.

To ensure the security of your account, we recommend you enable login protection and operation protection.

The account ID is a unique ID for Tencent Cloud. The collaborator you are adding needs to go to Account Center - Account Info to view the account ID.

4. Set permissions. You can set permissions for the created collaborator in any of the following three ways. After the collaborator is associated with a policy, they can get the permissions described in the policy.

Use group permissions: using groups is the best way to manage user permissions by job function. You can use group-associated permissions to grant permissions. Click **Use group permissions** and select the desired user group to add the collaborator to an existing or new user group. The collaborator will then be associated with the policies of the group.

Copy existing user policies: click **Copy existing user policies** and select the user whose permissions you want to use, and the new collaborator will be associated with the policies of the existing user.

Select policies from the policy list: click **Select policies from the policy list** and select the policies you want to associate with the collaborator.

5. Click **Done**.

Related Documents

For more information on how to log in as a collaborator, please see Logging in as Sub-account - Logging in as collaborator.

©2013-2022 Tencent Cloud. All rights reserved.

Setting Collaborator Permissions

Last updated：2024-01-23 17:31:59

Overview

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.

Directions

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 CAM Console and enter User List. Locate the collaborator to associate a policy with and click **Grant Permission** in the "Operation" column on the right.
2. Select one or more policies to be associated and click **OK**.

Association via group

You can add a user to a user group to automatically grant the user permissions included in the policies that are associated with the user group. The policy types obtained by the user in this method depend on the policies associated with the user group. If you need to disassociate the user from a policy that is associated with the user group, you must remove the user from the user group.

1. Log in to the CAM Console and enter User List. Locate the collaborator to associate a policy with and click **More** > **Add to Group** in the "Operation" column on the right.
2. Select one or more user groups to which you want to add the collaborator to and click **OK**.

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 CAM Console and enter User List. Locate the collaborator to disassociate a policy from and click the **username** of the collaborator to enter the collaborator details page.
2. Go to **Permissions** and locate the policy. Click **Disassociate** in the operation column on the right.
3. Click **OK** to complete the disassociation. This user will no longer have the permissions described in the policy.

Removing a collaborator from a group

©2013-2022 Tencent Cloud. All rights reserved.

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 CAM Console and enter User List. Locate the collaborator to disassociate a policy from and click the name of the collaborator to enter the collaborator details page.
2. Go to **Groups** and locate the group. Click **Remove from Group** in the operation column on the right.
3. Click **OK** to remove the collaborator from the user group and disassociate the user from the group-associated policy. After the removal, the collaborator will no longer have the permissions associated with the user group.

Collaborator Security Credentials

Collaborator Login

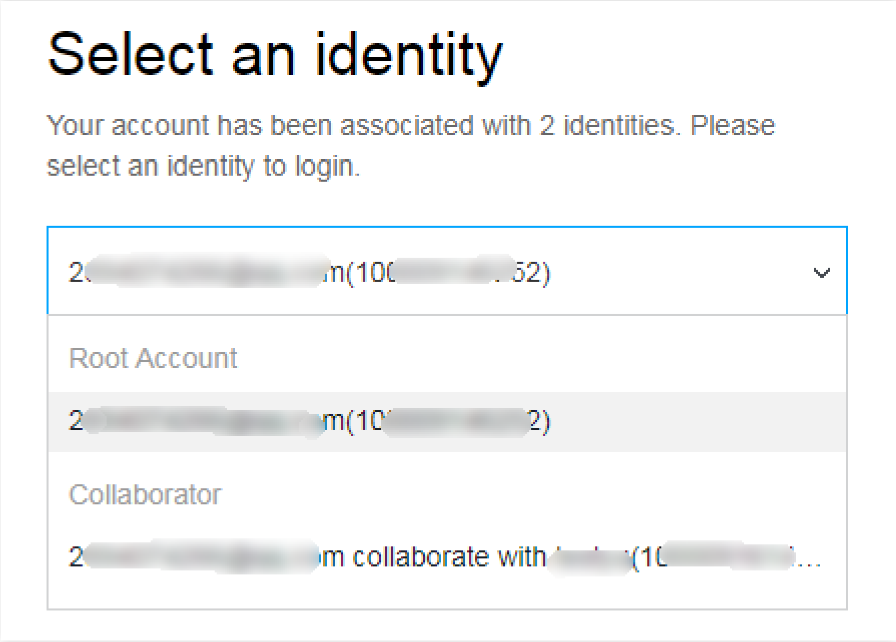
Last updated：2024-01-23 17:31:59

Introduction

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

Directions

1. Go to the Tencent Cloud account login page and select the added collaborator.
2. After entering the account information or scanning the code, go to the user identity selection page. See the following figure for reference:



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. In the user identity selection page, click ▼ on the right side of the account information. Select the root account identity that needs to be managed.
4. Click **Log in** to log in to the collaborator account.

©2013-2022 Tencent Cloud. All rights reserved.

Setting Security Protection for Collaborators

Last updated：2024-01-23 17:31:59

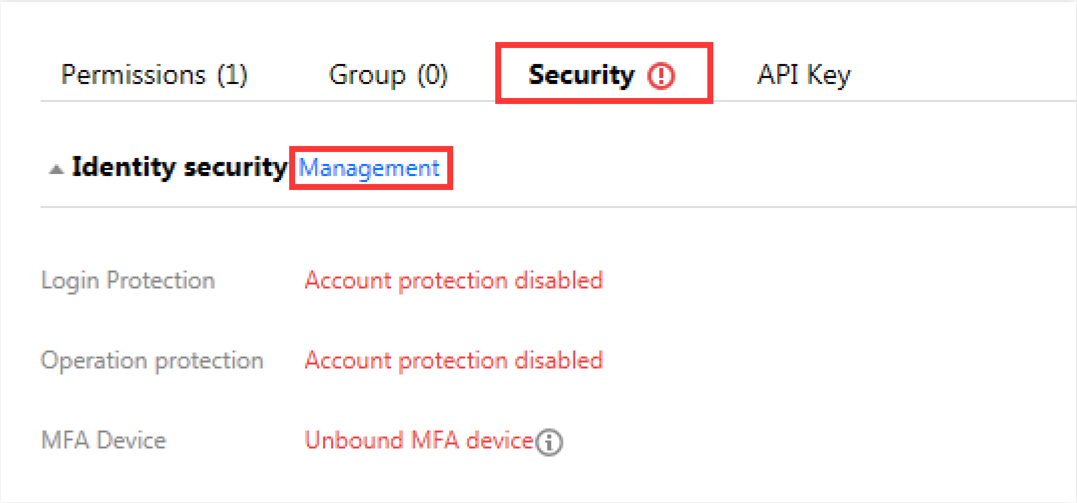
Introduction

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

Directions

Enabling security protection for collaborators

1. Log in to the CAM Console and select **User** > **User List** on the left sidebar.
2. On the User List management page, select the collaborator for whom to configure security protection.
3. Click the user name to go to **User Details**.
4. On the User Details page, click **Security** to go to the security management section.
5. Click **Manage** next to **Identity Security**. See the figure below for reference:



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 enable security protection for the collaborator.

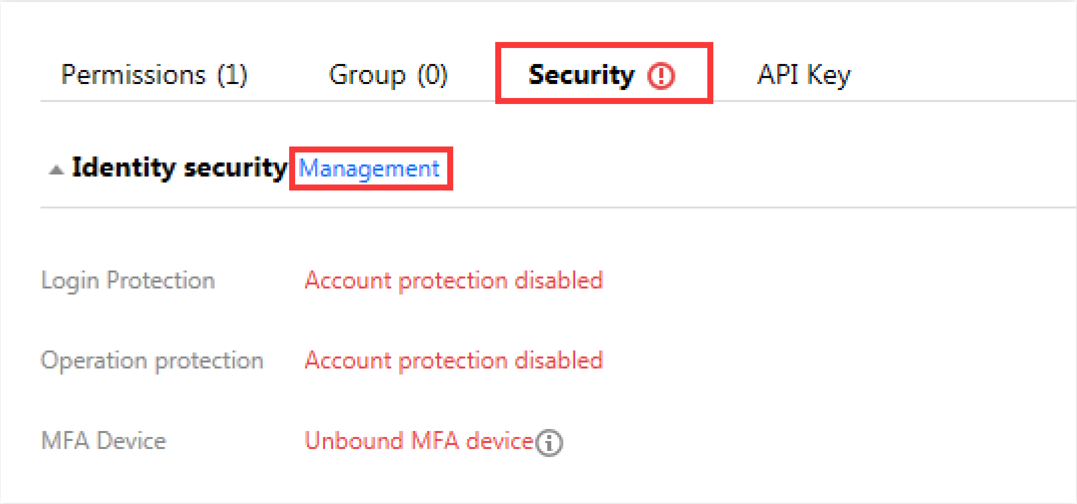
Note：

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

©2013-2022 Tencent Cloud. All rights reserved.

1. Log in to the CAM Console and select **User** > **User List** on the left sidebar.
2. On the User List management page, select the collaborator for whom to configure security protection.
3. Click the user name to go to **User Details**.
4. On the User Details page, click **Security** to go to the security management section.
5. Click **Manage** next to **Identity Security**. See the figure below for reference:



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 disable security protection for the collaborator.

Collaborator Message Subscriptions

Last updated：2024-01-23 17:31:59

Overview

This document describes how to verify message channels and set message subscriptions for a collaborator. The collaborator must first verify the message channels before they can receive messages. They will then receive subscribed messages through the verified message channels.

Directions

Verifying message channel

1. Log in to the CAM Console and select **User** > **User List** on the left sidebar.
2. On the user list management page, locate the collaborator to set the message subscription for.
3. Click the **username** to enter the user details page.
4. On the user details page, click **Send verification link** next to a user message channel.

Mobile: the system will send a verification message to the mobile number set for the collaborator. Click on the link in the message to verify this channel.

Email: the system will send a verification message to the email address set for the collaborator. Click on the link in the message to verify this channel.

Setting message subscription

1. Log in to the CAM Console and select **User** > **User List** on the left sidebar.
2. On the user list management page, locate the collaborator to set the message subscription for.
3. Click **More** > **Subscribe to Message** in the "Operation" column 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 **Confirm** to complete setting the message subscription.

Querying Collaborator Information

Last updated：2024-01-23 17:31:58

Overview

This document describes how to view collaborator information, such as user groups, message subscriptions, login protection, operation protection, MFA device status, and console access status, and how to search for collaborators by using keywords such as username, account ID, `SecretId` , mobile number, email, and notes.

Prerequisites

Log in to the CAM Console and enter User List.

Directions

Expanding to view collaborator information

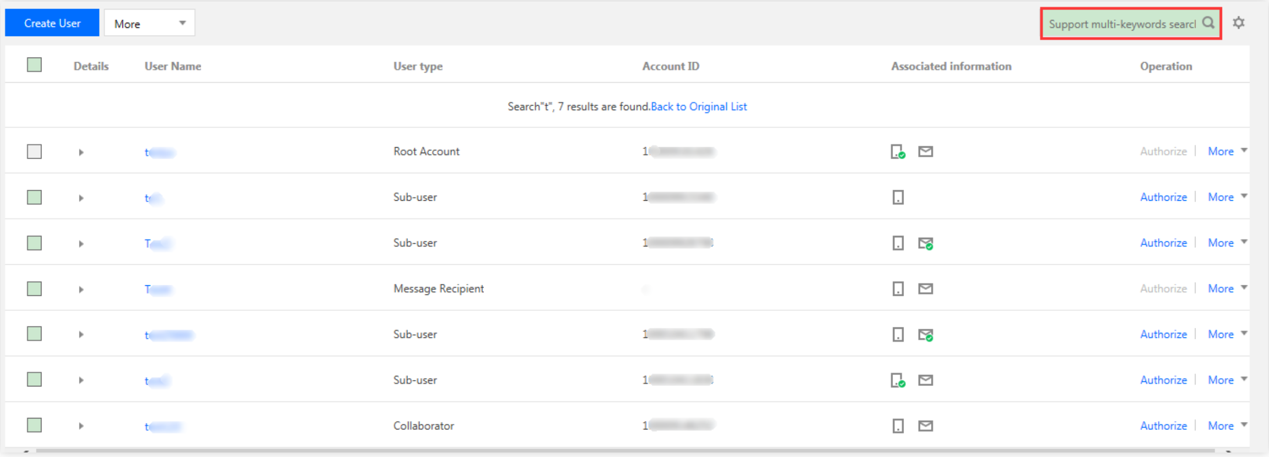
You can expand to view collaborator information, which includes user groups, message subscriptions, login protection, operation protection, MFA device status, and console access status.

1. On the user list management page, locate the collaborator that you want to view.
2. Click the details column icon (▶) on the left.
3. View the information of the collaborator in the expanded section.

Using search box to search for collaborator

You can search for collaborators by using keywords such as username, account ID, `SecretId` , mobile phone, email, or notes.

1. On the user list management page, locate the search box in the top-right corner.
2. In the search box, enter the keyword and click the search icon on the right to search for collaborators as shown below:



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

Deleting Collaborators

Last updated：2024-01-23 17:31:58

Introduction

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

Prerequisites

Log in to the CAM Console and go to the User List management page.

Directions

Deleting a single collaborator

1. In the **User List** management page, locate the collaborator that you want to delete.
2. Click **More** > **Delete** in the operations column on the right.
3. A **Delete User** window will pop up. Confirm that the collaborator’s API key has already been disabled and deleted. For more information, see Access Key.
4. Click **Delete** to delete the collaborator.

Deleting multiple collaborators

1. In the **User List** management page, select the collaborators that you want to delete.
2. Click **More** on the top left and select **Delete** from the dropdown menu.
3. A **Delete User** window will pop up. Confirm that the selected collaborators’ API keys have already been disabled and deleted. For more information, see Access Key.
4. Click **Delete** to delete the selected collaborators.

Switching Collaborator Identities

Last updated：2024-01-23 17:31:59

Overview

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.

Prerequisites

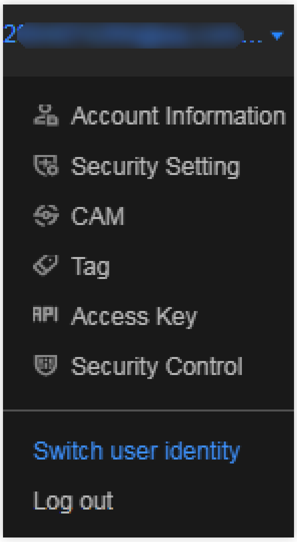
The logged-in account is a collaborator of another root account.

Note:

For more information on how to create a collaborator, please see Creating Collaborator.

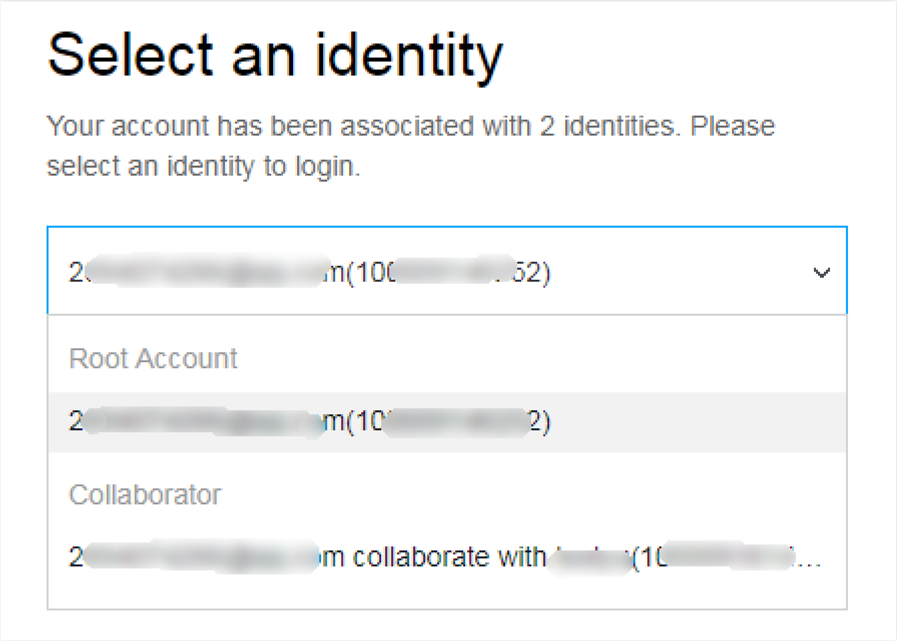
Directions

1. Go to the Tencent Cloud console and mouse over the account icon in the top-right corner of the page.
2. In the drop-down list that appears, click **Switch user identity** as shown below:



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

©2013-2022 Tencent Cloud. All rights reserved.



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]...

4. Click **Sign In** to switch the identity.

©2013-2022 Tencent Cloud. All rights reserved.

Message Recipients

Message Recipient Message Subscriptions

Last updated：2024-01-23 17:29:58

Introduction

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.

Prerequisites

Log in to the CAM console and go to the User List management page.

Directions

Verifying Message Channels

1. In the User List management page, locate the message recipient to set the message subscription for.
2. Click the user name to go to the user details page.
3. In the user details page, click **Complete Verification** next to the user message channels.

Mobile: The system will send a verification message to the mobile phone number set. After the user receives the verification message, they can click the confirmation link to verify the mobile message channel.

Email: The system will send a verification message to the email address set. After the user receives the verification message, they can click the confirmation link to verify the email message channel.

Receiving Messages on WeChat: When email verification is completed, the system will send an email containing a QR code to the email address set. The user can scan the QR code with WeChat to add WeChat as a message channel.

Setting Message Subscriptions

1. In the User List management page, locate the message recipient to set the message subscription for.
2. Click **More** > **Subscribe to Messages** in the operations column on the right.
3. A **Subscribe to Messages** window will pop up. You can select the message types here. Press ▼ to expand for granular selection options.
4. Click **OK** to complete setting the message subscription.

©2013-2022 Tencent Cloud. All rights reserved.

Setting Message Recipient User Groups

Last updated：2024-01-23 17:29:58

Overview

This document describes how to add/remove a message recipient to/from a user group to have them receive or stop receiving message notifications.

Prerequisites

Log in to the CAM Console and enter the User List management page.

Directions

Adding message recipients to user groups

You can add a message recipient to a 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 that you want to add to the user group.
2. Click **More** > **Add to Group** in the "Operation" column.
3. In the "Add to Group" window that pops up, select the user group you want to add the recipient to.
4. Click **OK** to add the user to the group.

Removing message recipients from user groups

You can remove a message recipient from a user group so that the recipient will no longer receive message notifications set for the group.

1. On the user list management page, locate the message recipient that you want to remove from the group.
2. Click the name of the message recipient to enter the user details page.
3. Go to **Group** and locate the target group.
4. Click **Remove from Group** > **OK** in the "Operation" column on the right to remove the message recipient from the user group.

©2013-2022 Tencent Cloud. All rights reserved.

Creating Message Recipient

Last updated：2024-01-23 17:29:58

Introduction

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.

Directions

1. Log in to the CAM Console and select **User** > **User List** in the left sidebar.
2. On the User List page, click **Create User**.
3. Click **Create a custom user**.
4. On the User Type page, click **Receive messages only**.
5. Enter a username, notes, a mobile phone number, and an email address. The notes are optional.
6. Click **Done** to complete the creation.

©2013-2022 Tencent Cloud. All rights reserved.

Deleting Message Recipients

Last updated：2024-01-23 17:29:58

Introduction

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.

Prerequisites

Log in to the CAM console and go to the User List page.

Directions

Deleting a Message Recipient

1. In the User List page, locate the message recipient that you want to delete.
2. Click **More** > **Delete** in the operation column on the right to delete a single message recipient.

Deleting Multiple Message Recipients

1. Select the message recipients that you want to delete by checking boxes on the left.
2. Click **More** and select **Delete** from the dropdown menu to delete selected message recipients.

User Information

Last updated：2024-01-23 17:35:43

Introduction

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

Viewing User Information

1. Log in to the CAM console and go to the User List management page. Find the sub-account whose user information you need to view.
2. Click the **user name** to go to the **user details** page.
3. On this page you can view the user information of the current sub-account, including user name, notes, mobile phone number, and email address.

Modifying User Information

1. Log in to the CAM console and go to the User List management page. Find the sub-account whose user information you need to modify.
2. Click the **user name** to go to the **user details** page. Click **Modify** in the upper right corner.
3. Edit the user information in the pop up box.
User name: you can modify the usernames for collaborators. the usernames of sub-users cannot be modified as they are used for signing in.
Notes: you can edit notes for sub-accounts.
Mobile phone number: you can modify the mobile phone number bound to the current sub-account. This phone number can be used to receive messages and notifications from the root account. It can also be used for identity verification before performing sensitive operations.
Email address: you can modify the email address bound to the current sub-account. This email can be used to receive messages and notifications from the root account.
4. Click **OK** to complete the modification of the user information. You can search for your sub-accounts by using the modified user name, mobile phone number, notes, or email address in the User List management page.

Related Documentation

©2013-2022 Tencent Cloud. All rights reserved.

For more information on sub-accounts message subscriptions, see Sub-Users Message Subscriptions, Collaborator Message Subscriptions, and Message Recipient Message Subscriptions.

User Settings

Password Rules

Last updated：2024-01-23 17:31:59

Background information

Your password is hashed by using Secure Hash Algorithm 256 (SHA-256) with a salt value. Tencent Cloud does not save your password in plaintext. This ensures password security.

Overview

This document describes how to modify the password rules for sub-users in the CAM console, including password complexity, length, and validity period. If you don't modify the password rules, the default settings will be applied.
In the following password setting scenarios, you need to follow the password rules that have been set:
If you select **Tencent Cloud console access** and **Customize password** when creating a sub-user.
If you select **Customize password** when resetting the login password for a sub-user.

Directions

1. Log in to the CAM console and select **Users** > User Settings on the left sidebar.
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 need to follow such rules when you reset the password next time.

Note:

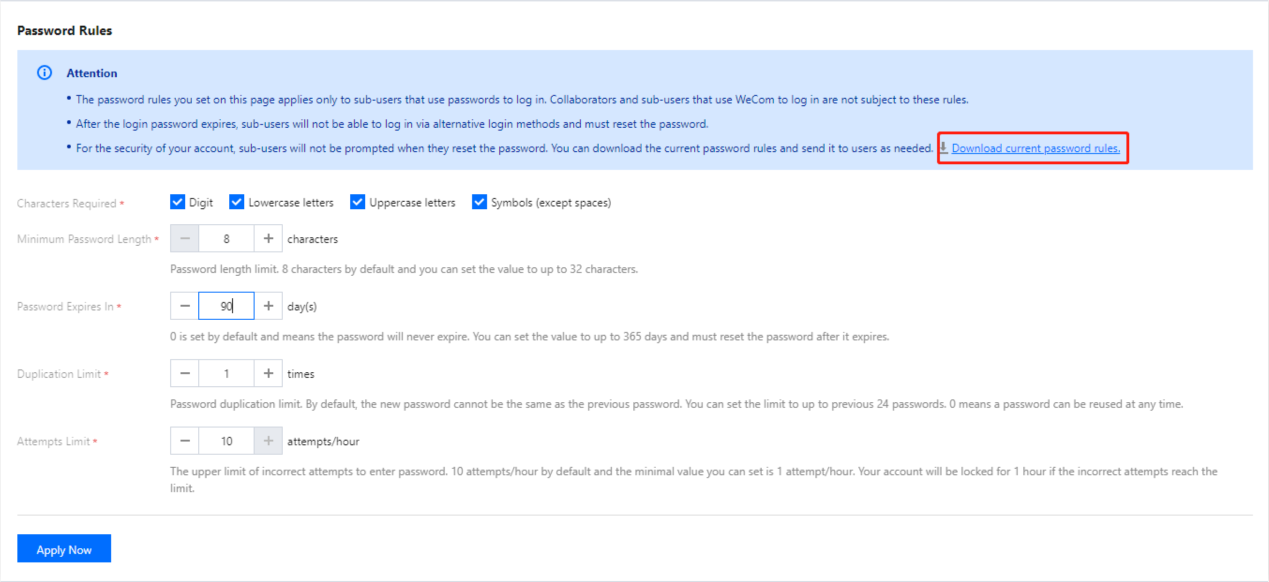
The password rules you set in this module apply only to sub-users who use passwords for login.

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, the password rules will not be prompted for sub-users when they reset the password.

The root account, admins, and sub-users with the `cam:GetPasswordRules` API permission can download the current password rules on the **Password Rules** page and pass them to users who need them, as shown below:

©2013-2022 Tencent Cloud. All rights reserved.



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.

Login Restrictions

Last updated：2024-01-23 17:31:58

Overview

This document describes how to set login restrictions for sub-accounts in the CAM console, so that they can log in to the Tencent Cloud console only in secure environments. Specifically, you can restrict suspicious logins (from unusual login locations or 30 days after the last successful login) and allow/forbid login from specified IPs.

Directions

IP restriction

Setting IP restriction

You can forbid sub-accounts to log in to the Tencent Cloud console by setting IP restriction. The sub-accounts can manage the resources of the root account under the restricted conditions.

1. Log in to the CAM console and enable **Login Restrictions** on the **Users** >**User Settings** page.
2. Select **IP Restriction**.
3. Set the IP type.

Allowlist: after you set up the allowlist, sub-accounts are allowed to log in to the console using the IPs (IP ranges) in the allowlist.

Blocklist: after you set up the blocklist, sub-accounts are not allowed to log in to the console using the IPs (IP ranges) in the blocklist.

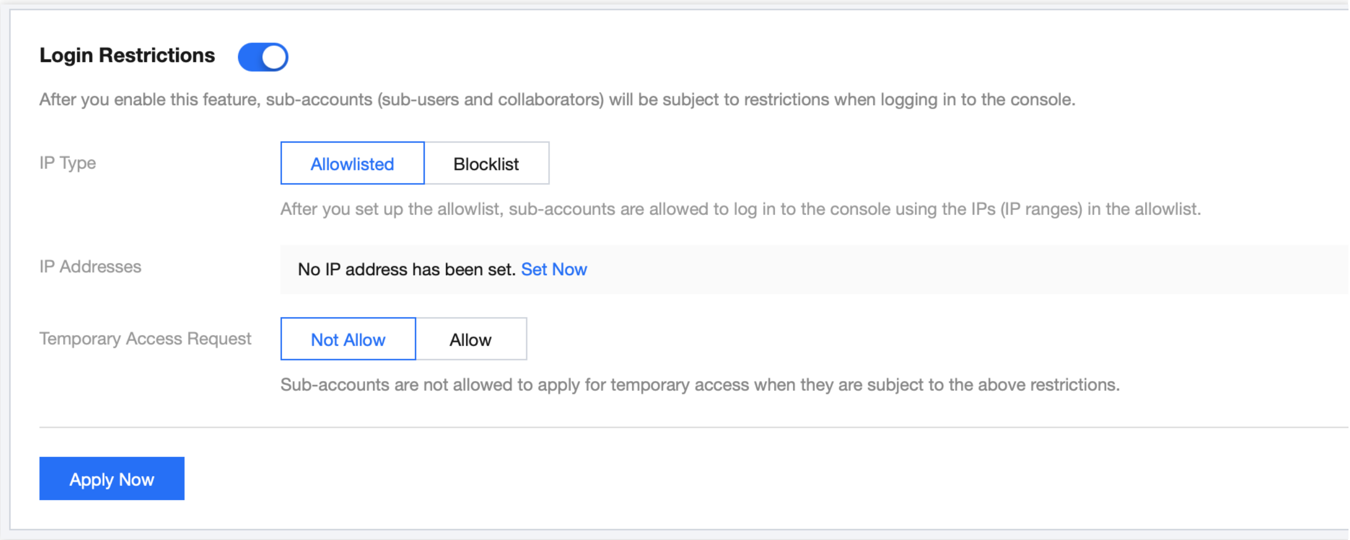
4. Configure IPs by clicking **Add**. You can add up to 10 restricted IPs.
5. Set temporary access request. This specifies whether sub-accounts are allowed to apply for temporary access when logging in to the console.

Not Allow: sub-accounts are not allowed to apply for temporary access when they are subject to the above restrictions.

Allow: sub-accounts are allowed to apply for temporary access when they are subject to the above restrictions. The applications will be sent to approvers for review via a valid message channel. If an application is approved, the sub-account will get a two-hour access to the console. If you select **Allow**, you need to click **Set Now** to set the approver.

6. Click **Apply Now**.

©2013-2022 Tencent Cloud. All rights reserved.



Login Restrictions

After you enable this feature, sub-accounts (sub-users and collaborators) will be subject to restrictions when logging in to the console.

IP Type: [✓ Allowlisted] Blocklist

After you set up the allowlist, sub-accounts are allowed to log in to the console using the IPs (IP ranges) in the allowlist.

IP Addresses: No IP address has been set. Set Now

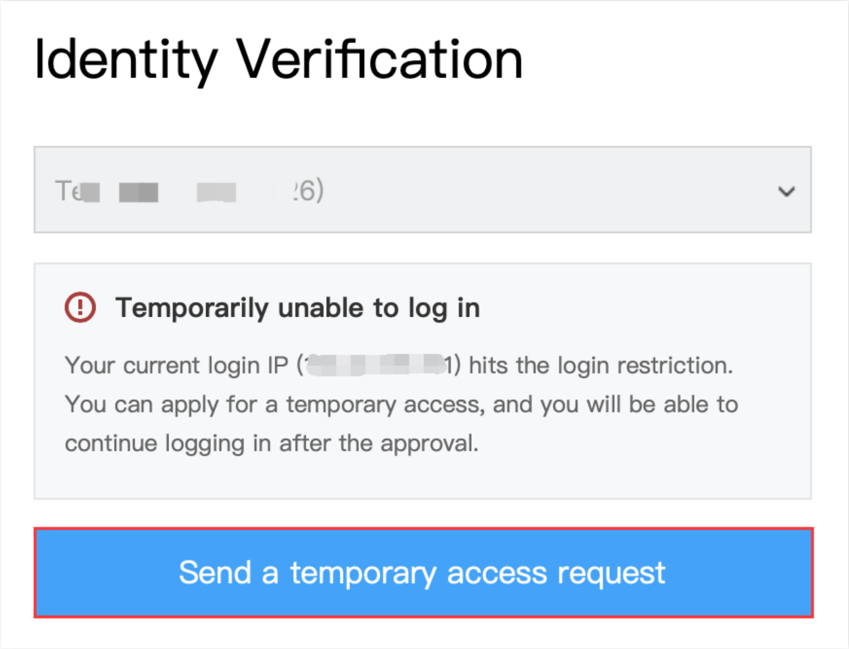
Temporary Access Request: [✓ Not Allow] Allow

Sub-accounts are not allowed to apply for temporary access when they are subject to the above restrictions.

Applying for temporary access from restricted IP

When a sub-account login hits the login IP restriction conditions, if temporary access request is allowed, the sub-account can apply for temporary access, and after the approver approves the request, they will get a two-hour access to the console.

1. When a sub-account login hits the login restrictions, the system will prompt that the sub-account cannot log in temporarily. They can click **Send Temporary Access Request** as shown below:



Identity Verification

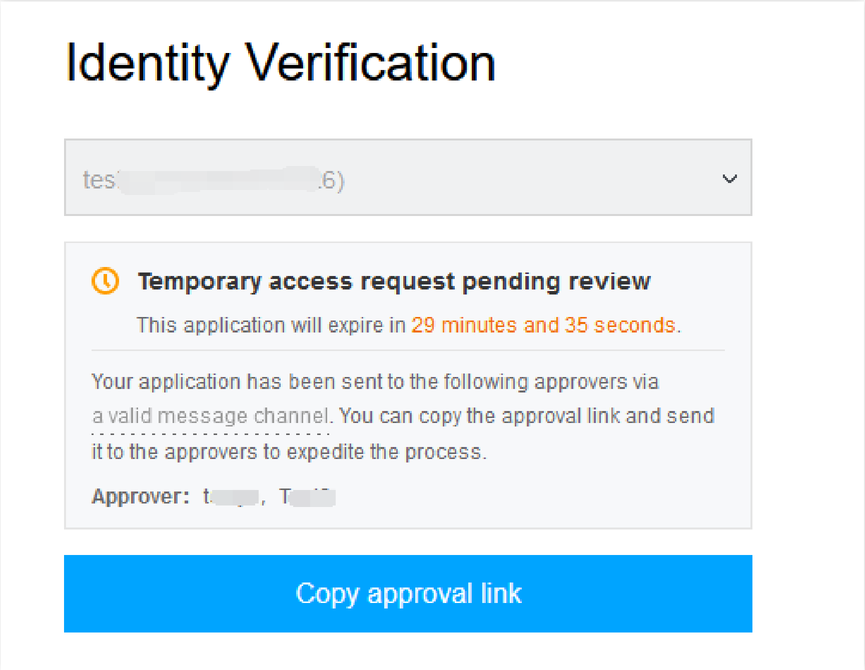
Te[redacted]6)

Temporarily unable to log in

Your current login IP ([redacted]1) hits the login restriction. You can apply for a temporary access, and you will be able to continue logging in after the approval.

2. The page will prompt that "The temporary access request is waiting for approval". The system will send the submitted request to the following approver through a valid message channel, and the request will be valid for 30 minutes. The sub-account can copy the review link and send it to the approver to expedite the processing, as shown below:

©2013-2022 Tencent Cloud. All rights reserved.



Identity Verification

tes[redacted]6)

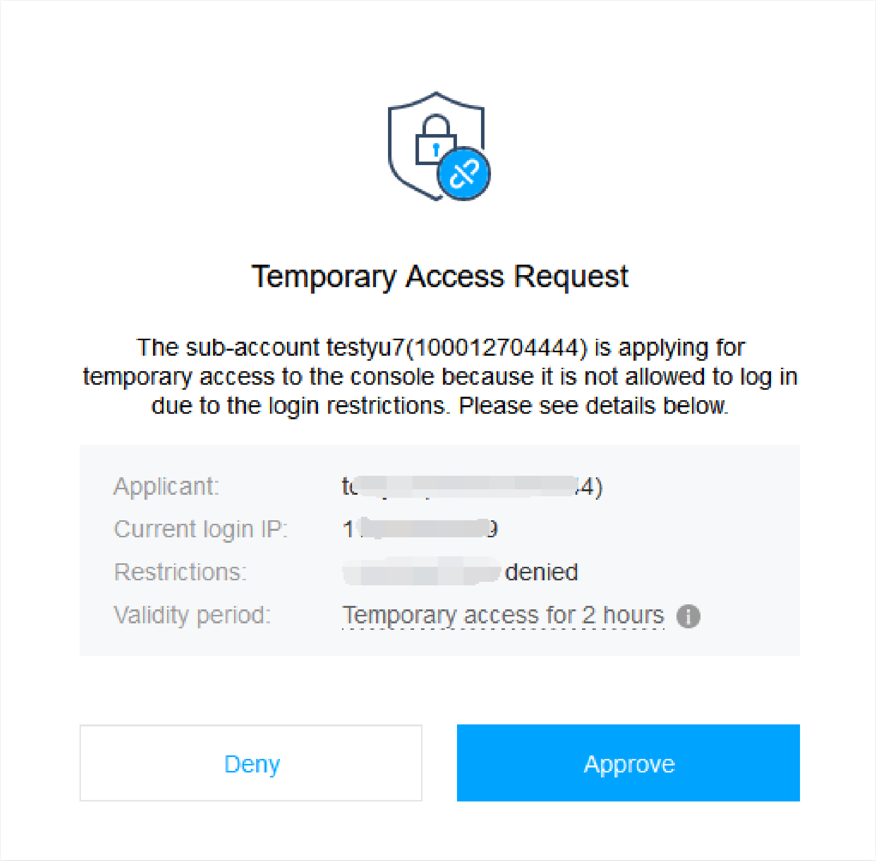
Temporary access request pending review

This application will expire in 29 minutes and 35 seconds.

Your application has been sent to the following approvers via a valid message channel. You can copy the approval link and send it to the approvers to expedite the process.

Approver: t[redacted], T[redacted]

3. The approver set in Login Restrictions will be able to approve or reject this request at the review link as shown below:



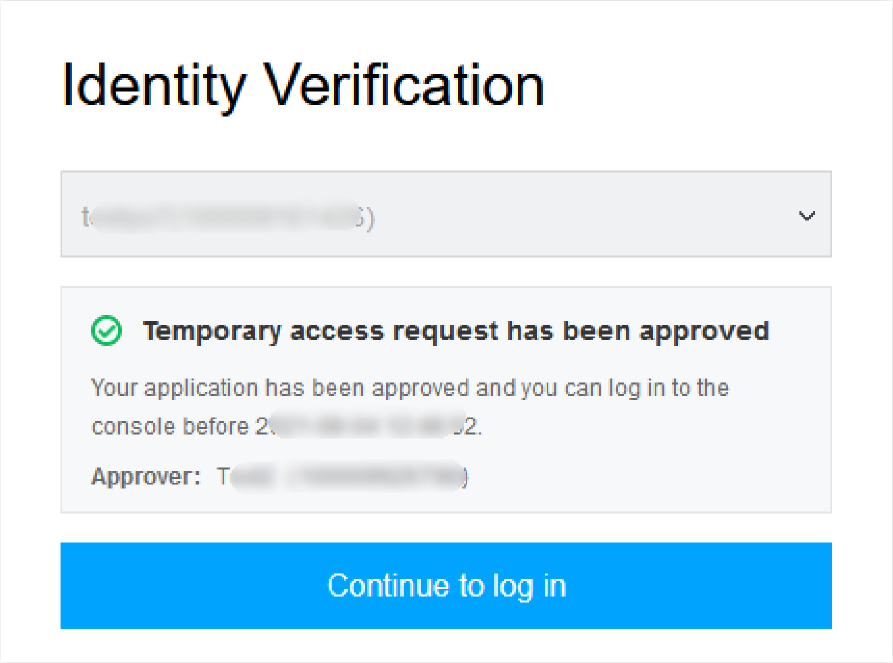
Temporary Access Request

The sub-account testyu7(100012704444) is applying for temporary access to the console because it is not allowed to log in due to the login restrictions. Please see details below.

Applicant:	t[redacted]4)
Current login IP:	1[redacted]9
Restrictions:	[redacted] denied
Validity period:	Temporary access for 2 hours

4. If the approver approves the request, the sub-account login UI will prompt that the temporary access request has been approved, and the sub-account can click **Proceed with Login** to get a two-hour access to the console as

shown below:



Identity Verification

t[redacted])

✓ Temporary access request has been approved

Your application has been approved and you can log in to the console before 2[redacted]2.

Approver: T[redacted])

5. If the approver rejects the request, the sub-account login UI will prompt that the temporary access request has been rejected. The sub-account can contact the approver before submitting a new request.

Advanced Settings

Last updated：2024-01-23 17:31:58

Overview

This document describes how to set the single login session expiration time for a sub-account in the CAM console. After the session times out, the sub-account needs to log in to the console again.

Directions

1. Log in to the CAM console and find **Advanced Settings** on the **Users** >**User Settings** page.
2. Set the duration in **Persistent Login Session Timeout for Sub-account**
3. Click **Save**.

©2013-2022 Tencent Cloud. All rights reserved.

Identity Provider

SSO Overview

Last updated：2024-01-23 17:42:59

Tencent Cloud supports Single Sign-On (SSO) that uses SAML 2.0 and OIDC protocols, allowing external users who have authenticated through an Identity Provider (IdP) to directly access your Tencent Cloud resources. Currently, Tencent Cloud supports two modes of SSO login: user-based SSO and role-based SSO.

Fundamental Concepts of SSO

Concept	Description
Identity Provider (IdP)	An entity that encompasses metadata about an external IdP, offering identity management services. On-Premise IdP: Microsoft Active Directory Federation Service (ADFS), Shibboleth, etc. Cloud-based IdP: Azure AD, Google Workspace, Okta, OneLogin, etc.
Service Provider (SP)	By using IdP's identity management function and the user's information supplied by IdP, the SP provides users with specific service applications. Some non-SAML protocol identity systems (for example: OpenID Connect) also refer to the SP as the trusted party of IdP.
Security Assertion Markup Language (SAML 2.0)	A criterion protocol for implementing enterprise-level user identification. It is one of the ways to facilitate communication between SP and IdP. SAML 2.0 has become a factual criterion for implementing enterprise-level SSO.
SAML Assertion	The core element in the SAML protocol used to describe the authentication request and response. For example, specific user attributes are included in the assertion of the authentication response.
Trust	A mutual trust mechanism established between an SP and an IdP, typically implemented through the use of public and private keys. The SP obtains the SAML metadata of the IdP in a trustworthy manner. The metadata contains the public key used for signature verification of SAML assertions issued by the IdP. The SP uses this public key to verify the integrity of the assertions.
OIDC	OIDC is an authentication protocol built upon OAuth 2.0. OAuth is an authorization protocol, and OIDC adds an identity layer on top of the existing OAuth protocol. Apart from the authorization capabilities provided by OAuth, it also allows the client to verify the identity of the end

	user and obtain the user's basic information through the OIDC protocol API (in the form of HTTP RESTful).
OIDC Token	OIDC can issue identity tokens that represent logged-in users, namely OIDC tokens. OIDC tokens are used to obtain basic information of the logged-in user.
Client ID	When your application registers with an external IdP, a client ID will be generated. This client ID is requisite when requesting the issuance of an OIDC token from the external IdP, and the issued OIDC token will also contain this client ID in the 'aud' field. During the setting up the OIDC IdP, the client ID will be configured. Tencent Cloud checks whether the client ID carried in the 'aud' field of the OIDC token is the same as that configured in the OIDC IdP when converting the OIDC token into an STS Token. The role can only be played when both IDs are identical.
Verification Fingerprint	To prevent Issuer URL from being maliciously hijacked or tampered with, you need to configure the verification fingerprint generated by the HTTPS CA certificate of the external IdP. Although Tencent Cloud will assist you in automatically calculating this fingerprint, it is recommended that you compute it locally (for instance, using OpenSSL to calculate the fingerprint), and contrast it with the fingerprint calculated by Tencent Cloud. If the comparison reveals differences, it indicates that the issuer URL might have been attacked. Please confirm again, and input the correct fingerprint.
IdP URL	OpenID Connect Identity Provider Identifier. Corresponds to the value of the "issuer" field in the OpenID Connect metadata document provided by the IdP.
Mapping Field	The field in the OpenID Connect IdP that maps to the Cloud Access Management (CAM) sub-user name. You can use the value of "claims_supported" in the OpenID Connect metadata document provided by the IdP. In this example, the name field maps to the CAM username.
Signature Public Key	Public key for verifying the OpenID Connect IdP ID Token signatures. Corresponds to the content (accessed by visiting the link) linked in the "jwks_uri" field of the OpenID Connect metadata document provided by the corresponding IdP. For the safeguarding of your account, it is advised to periodically rotate your signature public keys.

SSO Method

Tencent Cloud offers two types of SSO methods:

User-based SSO

Tencent Cloud determines the correspondence between enterprise users and CAM users through SAML assertions issued by the IdP. Enterprises can manage employee information in their local IdP, and employees can log in to Tencent Cloud through specified links. After logging in, enterprise users access Tencent Cloud resources using this CAM user. For more information, please refer to User-based SSO Overview.

Role-Based SSO

Tencent Cloud determines the correspondence between enterprise users and CAM users through SAML assertions or OIDC tokens issued by the IdP. After logging in, enterprise users access Tencent Cloud resources using this CAM user. It supports two types of role-based SSO based on SAML 2.0 and OIDC:

SAML Role-Based SSO: Tencent Cloud determines the CAM roles that enterprise users can utilise in Tencent Cloud through SAML assertions 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, please refer to Overview of SAML Role-Based SSO.

OIDC Role-Based SSO: Enterprise users use the OIDC tokens issued by the IdP, call Tencent's Application Programming Interface to impersonate a specified role and exchange for temporary role identity credentials (STS Token), and then use the STS Token to securely access Tencent Cloud resources. For more information, please refer to Overview of OIDC Role-Based Single Sign-On.

SSO Method Comparison

SSO Method	SP initiated SSO	IdP initiated SSO	Login with Sub-User Account and Password	Configuration of IdP Association with Multiple Tencent Cloud Accounts at a Time	Multiple IdPs
User-based SSO	Supported	Supported	Not supported	Not supported	Not supported
Role-based SSO	Not supported	Supported	Supported	Supported	Supported

©2013-2022 Tencent Cloud. All rights reserved.

Practical Scenarios for SSO

Last updated：2024-01-23 17:39:39

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

Role-Based SSO

Role-Based SSO applies to the following scenarios:

Considering management costs, you may prefer to avoid creating and managing users in the cloud, thus evading the workload brought about by user synchronization.

You want to sustain some cloud based local users while using SSO. The cloud based user can direct log in to Tencent Cloud and can be employed for a variety of purposes such as testing new features, serving as an alternative login method in the case of network or enterprise's IdP issues.

You want to differentiate permissions on the cloud based on the group joined by the user in the local IdP or a particular attribute of the user. You can adjust permissions by simply changing the group or attribute.

You assert multiple Tencent Cloud accounts but operate with a unified enterprise IdP. You desire a single configuration within the enterprise IdP that grants SSO capability to multiple Tencent Cloud accounts.

Your various branch offices contain multiple IdPs, and they all require access to a single Tencent Cloud account. You need to set up multiple IdPs within a single Tencent Cloud account to implement SSO.

You wish that SSO can also be performed through a programmatic access method except the console.

User-based SSO

User-based SSO applies to the following scenarios:

You prefer logins initiated on Tencent Cloud's login page, rather than directly accessing your IdP's login page.

There are certain cloud products you require that temporarily do not support role access. For the cloud products that support role access (i.e., access via STS), please refer to CAM-Enabled Role.

Your IdP does not support sophisticated customized attribute configurations.

Your business does not require role-based SSO but you wish to streamline the IdP configurations.

©2013-2022 Tencent Cloud. All rights reserved.

User-Based SSO

Overview of User-Based SSO

Last updated：2024-01-23 17:39:39

Overview

Tencent Cloud is the service provider (SP) and the enterprise is the identity provider (IdP) when they collaborate to implement user-based single sign-on (SSO). The user-based SSO allows an enterprise employee to access Tencent Cloud resources as a CAM sub-user.

Directions

Configuration process

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.
Purpose: to establish Tencent Cloud's trust in your IdP.
Steps: please see Configuring SAML in Tencent Cloud.
2. Configure Tencent Cloud as a trusted SP in your IdP and configure the SAML assertion attributes.
Purpose: to establish your IdP's trust in Tencent Cloud.
Steps: please see Configuring SAML in IdP.
3. Log in to the CAM console or call an API to create a CAM sub-user with the same name as that in the IdP.
Purpose: to use sub-users for subsequent logins.
Steps: please see Creating Sub-user.

Login and verification process

After user-based SSO is configured, the enterprise employee (for example, "user1") in IdP can log in to Tencent Cloud console and access the resources he or she has permission to access with the steps below:

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.

©2013-2022 Tencent Cloud. All rights reserved.

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 SAML in Tencent Cloud

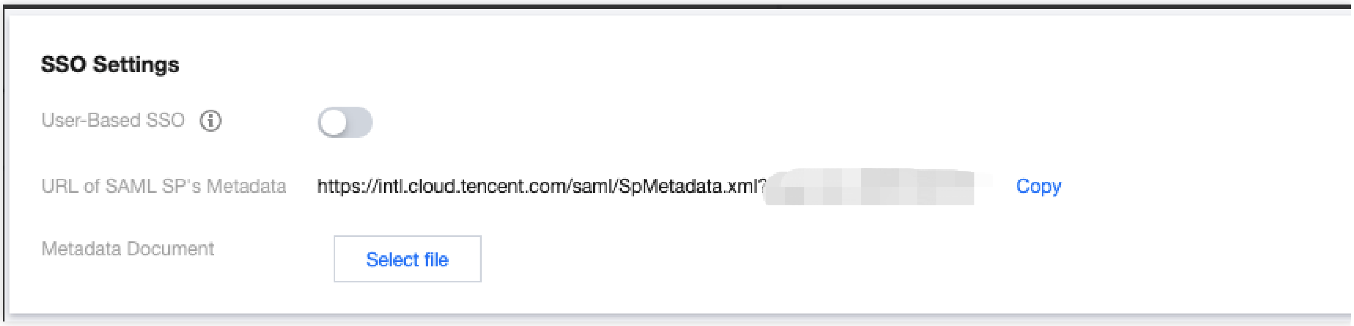
Last updated：2024-01-23 17:39:39

Overview

To make sure that a user in your IdP can log in to Tencent Cloud (the SP) via user-based SSO, you need to configure SAML for the IdP in Tencent Cloud to make Tencent Cloud trust your IdP.

Directions

1. Log in to the CAM console with your Tencent Cloud account.
2. On the left sidebar, click **Identity Providers** > **User-Based SSO**.
3. On the user-based SSO management page, you can view the user-based SSO status and the configuration information.



SSO Settings

User-Based SSO ⓘ ○

URL of SAML SP's Metadata https://intl.cloud.tencent.com/saml/SpMetadata.xml?[redacted] Copy

Metadata Document Select file

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

When user-based SSO is enabled: CAM sub-users cannot log in to Tencent Cloud via account ID and password. All CAM sub-users will be redirected to the IdP user login page for identity verification.

When user-based SSO is disabled: CAM users can login to Tencent Cloud via account ID and password, and the user-based SSO settings will not take effect.

5. Click **Select File** to upload the metadata file provided by your IdP. If you want to upload another file to replace the uploaded one, click **Upload Again**.

Note:

Your IdP provides the metadata file (typically in XML format). It contains the login URL as well as an X.509 public key certificate for verifying the validity of the IdP's SAML assertion.

If your IdP only provides the access address of the metadata, you can copy the address to the browser to open it. Then you can save the metadata as an XML file and upload it.

©2013-2022 Tencent Cloud. All rights reserved.

Configuring OIDC in Tencent Cloud SP

Last updated：2024-01-23 17:39:39

Overview

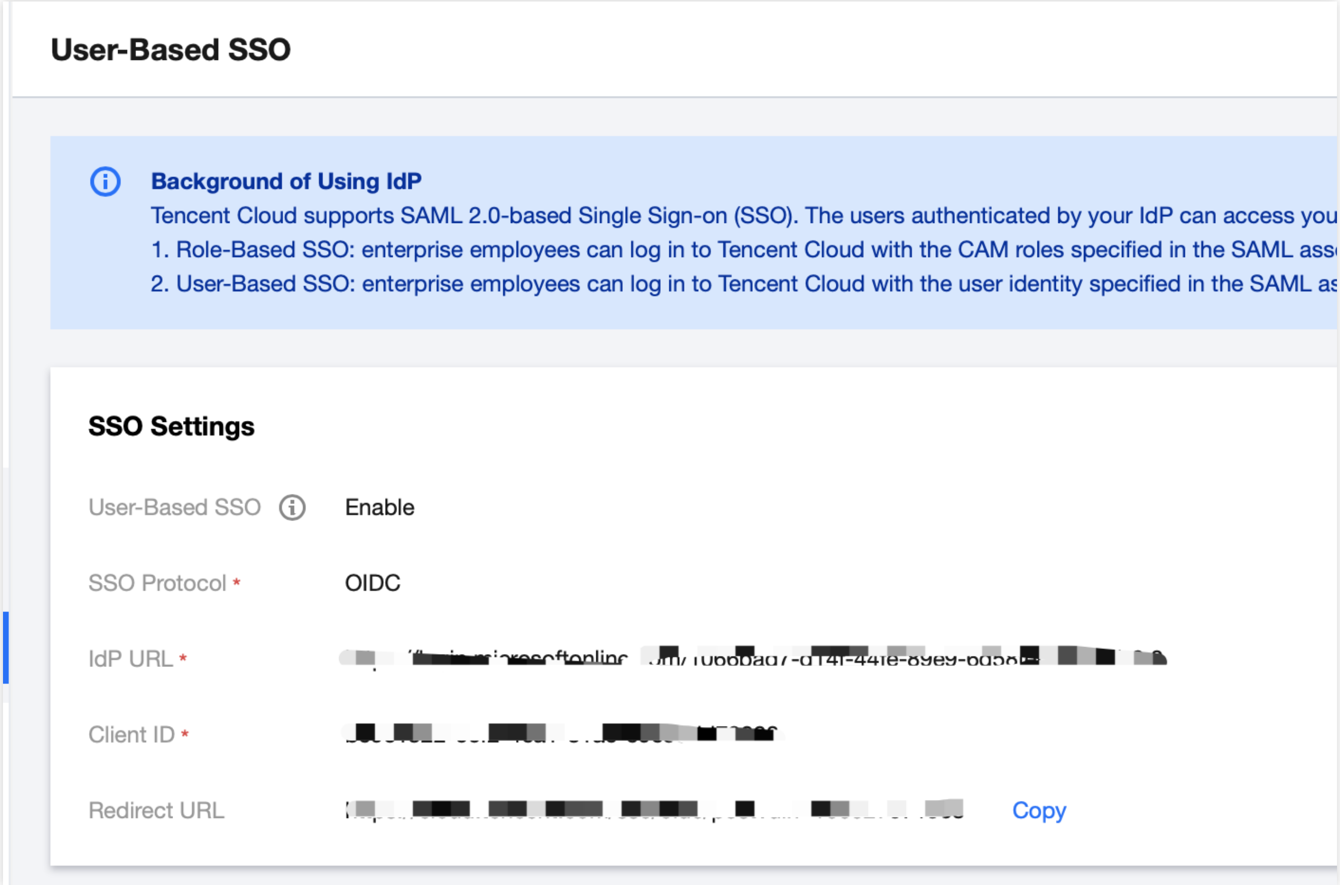
As the SP, Tencent Cloud needs to configure the OIDC for the IdP to establish a trust relationship with the enterprise IdP. This enables users from the enterprise IdP to log in to Tencent Cloud via user-based SSO.
This document uses Azure Active Directory as an example of IdP.

Note

View the OIDC protocol configuration information, (Copy the link at Azure Active Directory > App Registration > Endpoints > OpenID Connect Metadata Document, and open it in browser for specific configuration details)

Directions

1. Log in to the Tencent Cloud account Cloud Access Management Console.
2. In the navigation pane on the left, click **Identity Providers** > **User-Based SSO**.
3. On the User-Based SSO Management page, you can view the current User-Based SSO status and 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

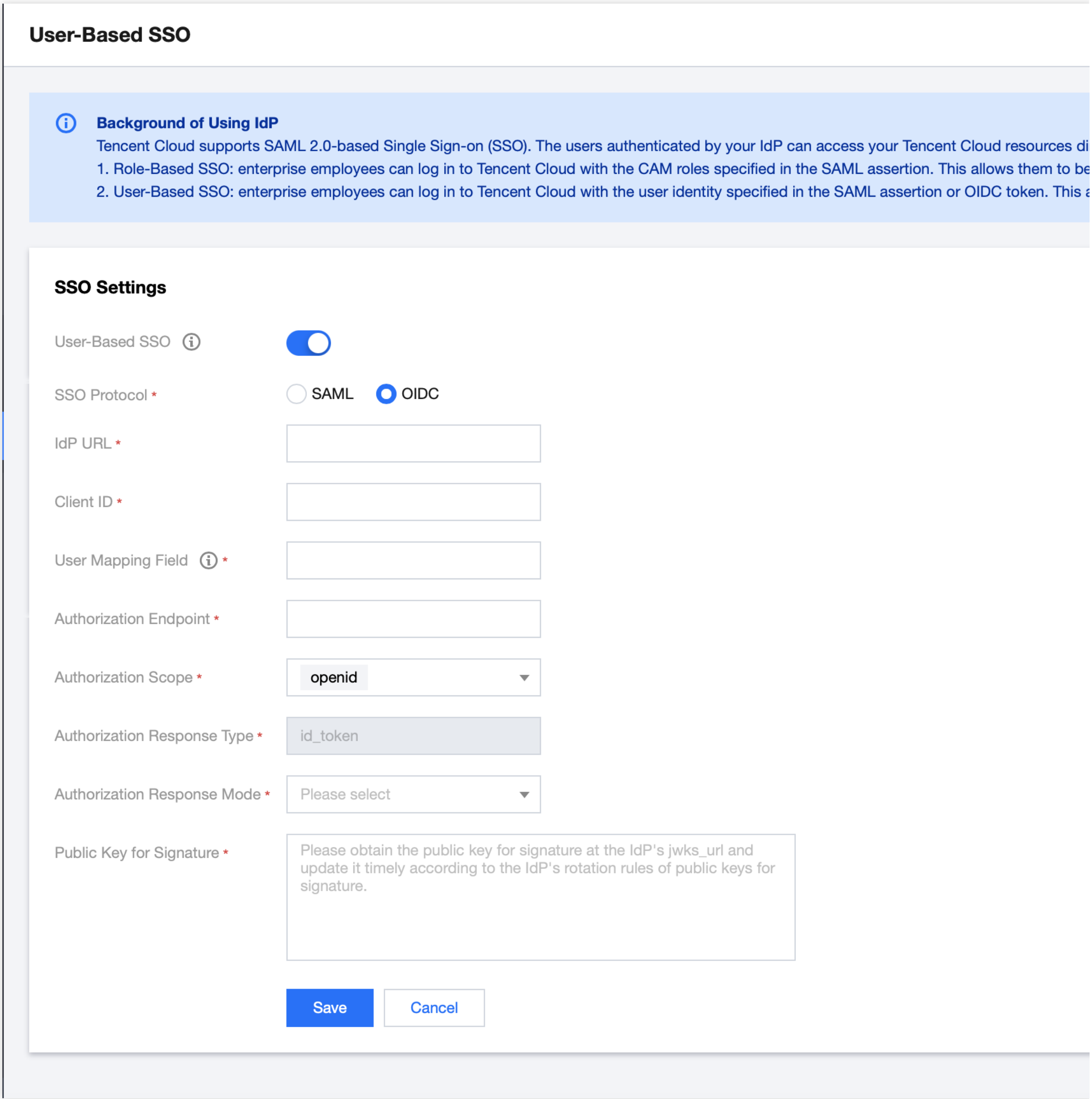
SSO Protocol * OIDC

IdP URL * [redacted]

Client ID * [redacted]

Redirect URL [redacted] Copy

4. By clicking on the switch button following User-Based SSO, you can either enable or disable 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 di

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

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 a

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 user-based SSO is enabled: CAM sub-users cannot log in to Tencent Cloud via account ID and password. All CAM sub-users will be redirected to the IdP user login page for identity verification.

When user-based SSO is disabled: CAM users can login to Tencent Cloud via account ID and password, and the user-based SSO settings will not take effect.

SSO Protocol: Select the OIDC type.

IdP URL: Identifier of OpenID Connect IdP. Corresponds to the 'issuer' field value in the OpenID Connect metadata document provided by the IdP.

Client ID: Client ID registered with the OpenID Connect IdP. It can be obtained from the **Azure Active Directory > Enterprise Applications > OIDCSSO Application Overview page**.

User Mapping Field: The field maps the CAM sub-user name in the OpenID Connect IdP. Optional values in the "claims_supported" provided in the OpenID Connect metadata document obtained from the IdP. In this example, the name field is used to map the CAM's username.

Authorization Request Endpoint: The address of the authorization request of the OpenID Connect IdP. Corresponds to the "authorization_endpoint" field value in the OpenID Connect metadata document provided by the IdP.

Authorization Request Scope: The range of information for the authorization request by the OpenID Connect IdP. By default, 'openid' is mandatory.

Authorization Request Response Type: The type of parameters returned by the authorization request from OpenID Connect IdP. By default, 'id_token' is mandatory.

Authorization Request Response Mode: The response mode of the authorization request by OpenID Connect IdP. 'form_post' and 'fragment' modes are optional, and 'form_post' is recommended.

Signature Public Key: The public key for verifying the signature of the OpenID Connect IdP ID Token. Corresponds to the content (obtained by visiting the link) linked in the "jwks_uri" field in the OpenID Connect metadata document provided by the IdP. For the security of your account, we recommend you to routinely rotate the signing public key.

5. Click Save.

©2013-2022 Tencent Cloud. All rights reserved.

Configuring SAML in IdP

Last updated：2024-01-23 17:39:39

To make sure that a user in the enterprise’s identity system (your IdP) can log in to Tencent Cloud (the SP) via user-based SSO, you need to configure SAML for Tencent Cloud in IdP to make your IdP trust Tencent Cloud.

Configuration process

1. Obtain the URL of SAML SP's metadata from Tencent Cloud.

1.1 Log in to the CAM console by using a Tencent Cloud account.

1.2 On the left sidebar, click **Identity Providers** > **User-Based SSO**.

1.3 On the user-based SSO management page, you can view or copy the URL of the metadata provided by the current user’s SAML SP.

2. Create an SAML SP in your IdP and configure Tencent Cloud as the reliable SP by using the methods below according to the actual situation of your IdP:

2.1 **If your IdP supports URL-based configuration:** copy the SAML SP metadata URL of Tencent Cloud in step 1 to your IdP.

2.2 **If your IdP supports configuration based on the uploaded file:** copy the SAML SP metadata URL of Tencent Cloud in step 1 to the browser and open it, save the metadata as an XML file, and upload the file to your IdP.

2.3 **If your IdP does not support the two methods above:** configure the parameters below in your IdP:

2.3.1 `Entity ID` : the value of the `entityID` attribute in the `EntityDescriptor` element of the downloaded metadata file.

2.3.2 `ACS URL` : the value of the `Location` attribute in the `AssertionConsumerService` element of the downloaded metadata file.

©2013-2022 Tencent Cloud. All rights reserved.

Configure OIDC In the Enterprise IdP

Last updated：2024-01-23 17:39:39

Overview

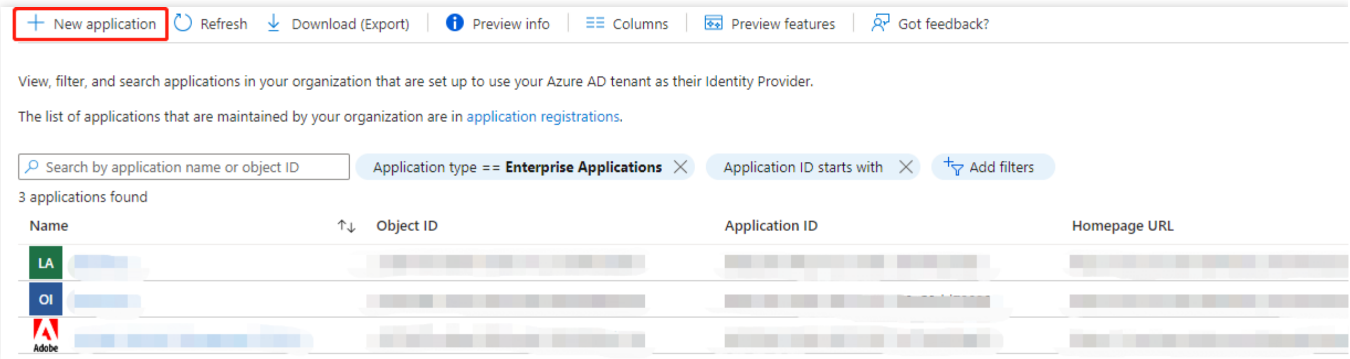
It's crucial for an enterprise's existing identity system - as an IdP - to configure OIDC for Tencent Cloud (the SP). This establishes trust from the enterprise IdP towards Tencent Cloud, enabling enterprise IdP users to log in to Tencent Cloud using user-based SSO.

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

Directions

Creating an Application in Enterprise IdP

1. Log in to the Azure Active Directory portal as an administrator.
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?
Search by application name or object ID
Application type == Enterprise Applications
Application ID starts with
Add filters

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

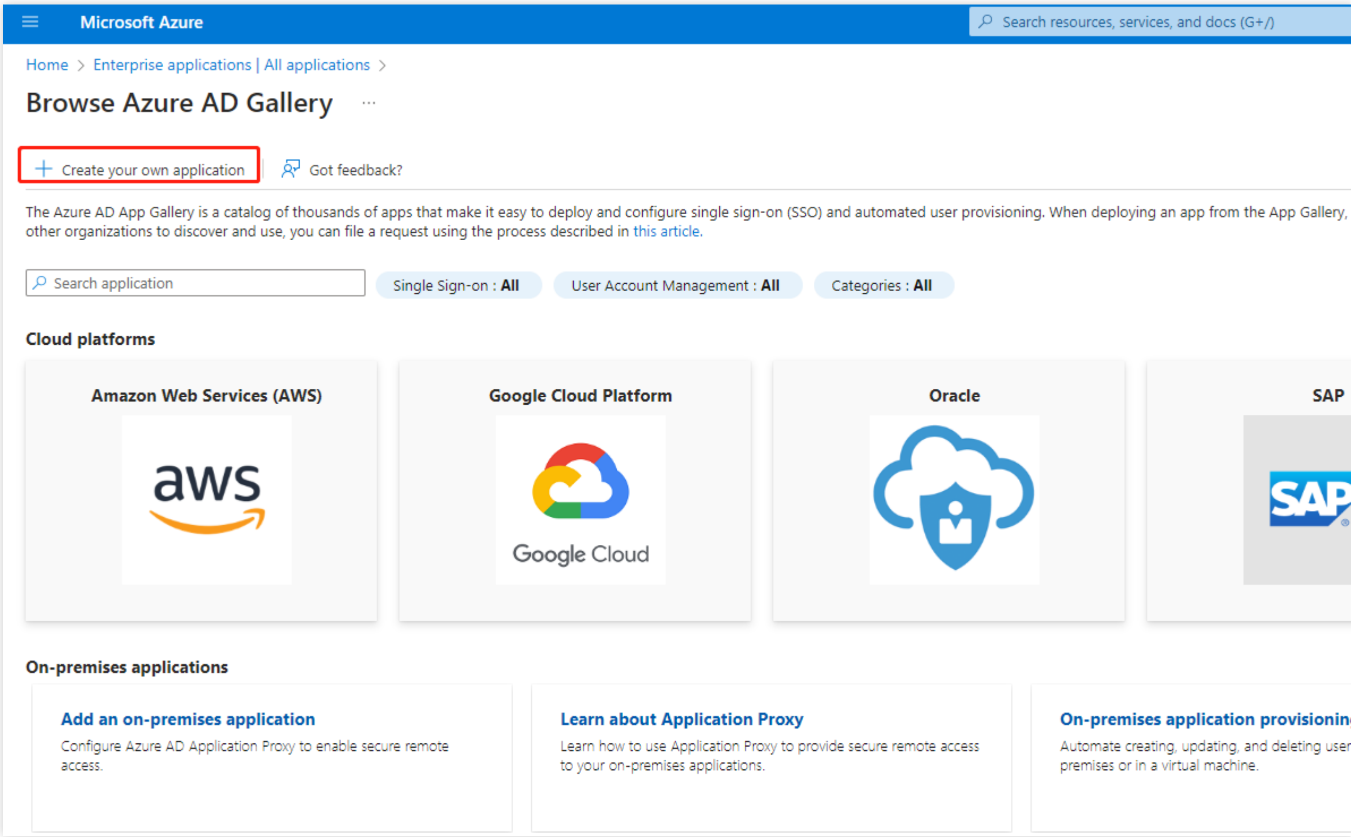
The list of applications that are maintained by your organization are in application registrations.

3 applications found

Name	Object ID	Application ID	Homepage URL
LA [redacted]	[redacted]	[redacted]	[redacted]
OI [redacted]	[redacted]	[redacted]	[redacted]
Adobe [redacted]	[redacted]	[redacted]	[redacted]

4. Click **Create Your Own Application**.

©2013-2022 Tencent Cloud. All rights reserved.


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, other organizations to discover and use, you can file a request using the process described in this article.

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
SAP
On-premises applications
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 provisionin
Automate creating, updating, and deleting user premises or in a virtual machine.

5. In the pop-up window on the right, enter the application name and select any additional applications not found in your current collection (non-database).

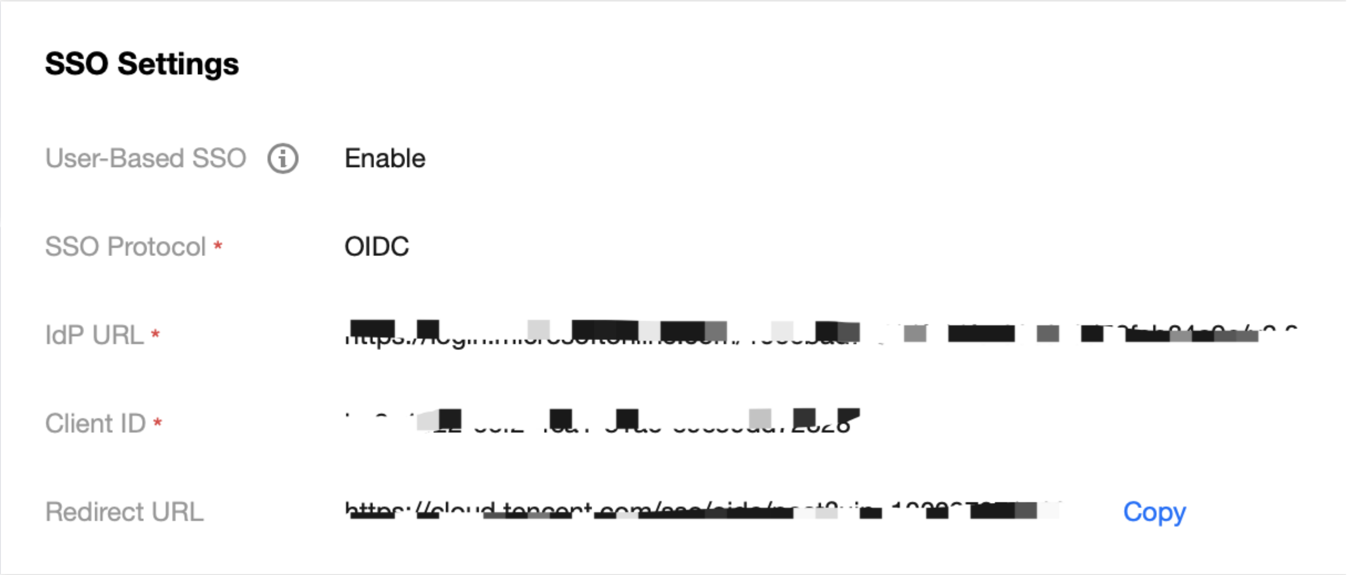
Obtaining the URL for the Metadata of the OIDC Service Provider from Tencent Cloud

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

Please Note:

For steps on Tencent Cloud's OIDC configuration, please refer to Configuring OIDC in Tencent Cloud SP.

2. In the left navigation bar, select **Identity Provider** > **User SSO**, as detailed below:



SSO Settings

User-Based SSO ⓘ Enable

SSO Protocol * OIDC

IdP URL * [redacted]

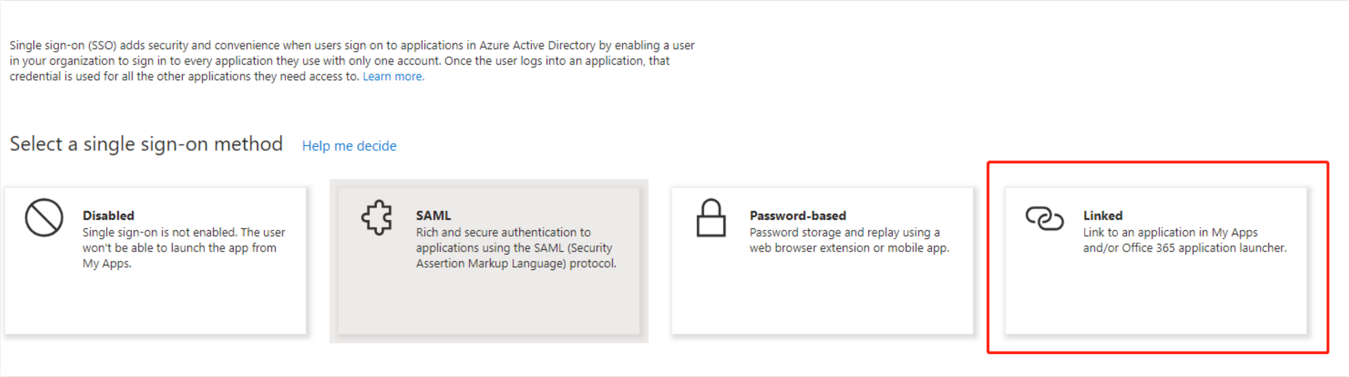
Client ID * [redacted]

Redirect URL [redacted] Copy

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

Incorporating the Redirect URL Obtained from Tencent Cloud to the Enterprise IdP

1. Navigate to Azure Active Directory> **App Registrations** > **All Applications**.
2. At the application name field, click the application that has been created.
3. In the left navigation bar, click on **Single Sign-On**.
4. Select link for the SSO method, as shown in the figure:



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

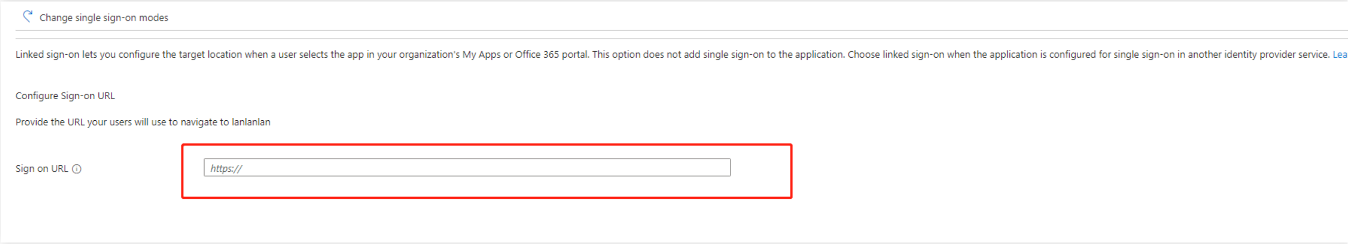
Disabled Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

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. Lea

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

Last updated：2024-01-23 17:46:24

If you already have an account system for your organization, you can use the Identity Provider (IdP) feature to allow your organization members to access Tencent Cloud resources. This eliminates the need to create a CAM sub-user for each organization member. With IdP, you can also manage non-Tencent Cloud identities and grant them permissions to access your Tencent Cloud resources whenever needed.

A known IdP can verify external identities on your behalf, so there is no need to implement custom login code or authentication. Users with authenticated external identities can use a role to log in to Tencent Cloud. You can grant the IdP role permissions to use your Tencent Cloud resources within the limited authorization range. External users log in to Tencent Cloud by using roles and roles use temporary keys, which helps prevent security problems caused by persistent keys (such as TencentCloud API keys), because such keys makes key rotation difficult and may result in credential leakage.

Use Cases

If you already have an account and user system for your organization, you can use the IdP feature of CAM to allow your users to access Tencent Cloud resources. This eliminates the need to create a CAM sub-user for each organization user. With the IdP feature, you can manage non-Tencent Cloud users and use the role feature to specify permissions to access Tencent Cloud resources for users whose identities are federated from an IdP.

Features

No need to create Tencent Cloud accounts

You don't need to create a Tencent Cloud account for each member in your organization, which helps avoid security issues caused by leakage of persistent access credentials (such as TencentCloud API keys) assigned to users.

Federated single sign-on (SSO)

If you already have your own organizational authentication system, you can easily implement federated SSO by leveraging an IdP.

Simplified login authentication process

With login codes provided by IdPs, identity federation with Tencent Cloud for enterprise customers is made simple and cost-effective.

Overview of SAML Role-Based SSO

Last updated：2024-01-23 17:46:25

During role-based SSO with Tencent Cloud, Tencent Cloud acts as the SP, while the enterprise's own identity management system serves as the 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 program.

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. Access the IdP's login page through a browser and select Tencent Cloud as the target service.
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 the 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. Then log in to the Tencent Cloud console with the specified CAM role.

Accessing Tencent Cloud Through a Program

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 through a program.
2. The IdP generates a SAML response containing a SAML assertion about the logged-in user and returns this response to the program.
3. The program invokes the APIAssumeRoleWithSAML provided by Tencent Cloud STS service and passes 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 verifies the SAML assertion and returns a temporary security credential to the program.
5. The program uses the temporary security credentials to call Tencent Cloud APIs.

©2013-2022 Tencent Cloud. All rights reserved.

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-based SSO can only be performed after these configurations are completed.

1. To establish a trust relationship between Tencent Cloud and the enterprise IdP, it is necessary to configure the enterprise IdP in Tencent Cloud. For more information, please refer to Creating a SAML IdP.
2. Enterprises need to create a CAM role for SSO in the Cloud Access Management Console or through programs and grant the necessary permissions. For more information, see Creating Role.
3. To establish a trust relationship between the enterprise IdP and Tencent Cloud, it is necessary to configure Tencent Cloud as a trusted SAML SP in the enterprise IdP and set the SAML assertion attributes.

Parameter Configuration Sample Code

Azure Active Directory Single Sign-On

©2013-2022 Tencent Cloud. All rights reserved.

Overview of OIDC Role-Based Single Sign-On

Last updated：2024-01-23 17:48:51

OIDC is an authentication protocol built on OAuth 2.0. Tencent Cloud CAM supports OIDC role-based SSO.

Basic Concepts

Concept	Note
OIDC	OIDC is an authentication protocol built on 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, OIDC 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 on behalf of logged-in users to applications, known as OIDC tokens. OIDC tokens are used to retrieve the basic information of the logged-in user.
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 customized validity 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, conform to the standard URL format. But 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 issued from an external IdP, you must use this client ID. The issued OIDC token will also carry this client ID in the 'aud' field. During the creation of an OIDC idP, this client ID is configured. Then, when using the OIDC token to exchange for an STS Token,

©2013-2022 Tencent Cloud. All rights reserved.

	Tencent Cloud verifies whether the client ID carried in the 'aud' field of the OIDC token matches that configured in the OIDC IdP. 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 there is no adequate security measures in place and the AccessKey is leaked. To address this issue, some enterprises register their applications with their own or third-party IdP that support OIDC (such as Google G Suite or Okta), to generate OIDC tokens for the applications using the capabilities of the OIDC IdP. In this scenario, with the role-based SSO capability provided by Tencent Cloud CAM, enterprise applications can exchange their OIDC tokens for Tencent Cloud temporary identity credentials (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 sites). If these websites support the generation of OIDC tokens, Tencent Cloud CAM can be used to accomplish SSO 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 IdP to establish a trust relationship between Tencent Cloud and the external IdP. For specific operations, please refer to Creating an OIDC Identity Provider.
3. In Tencent Cloud CAM, create the OIDC IdP's CAM role and authorize it. For specific operations, please refer to Creating Role.
4. Issue an OIDC token in the external IdP.
5. Use the OIDC Token to exchange for an STS Token. For specific operations, please refer to AssumeRoleWithWebIdentity.
6. Access Tencent Cloud resources using the STS Token.

Parameter Configuration Sample Code

Azure Active Directory Single Sign-On

SAML 2.0-Based Federation

Last updated：2024-01-23 17:46:25

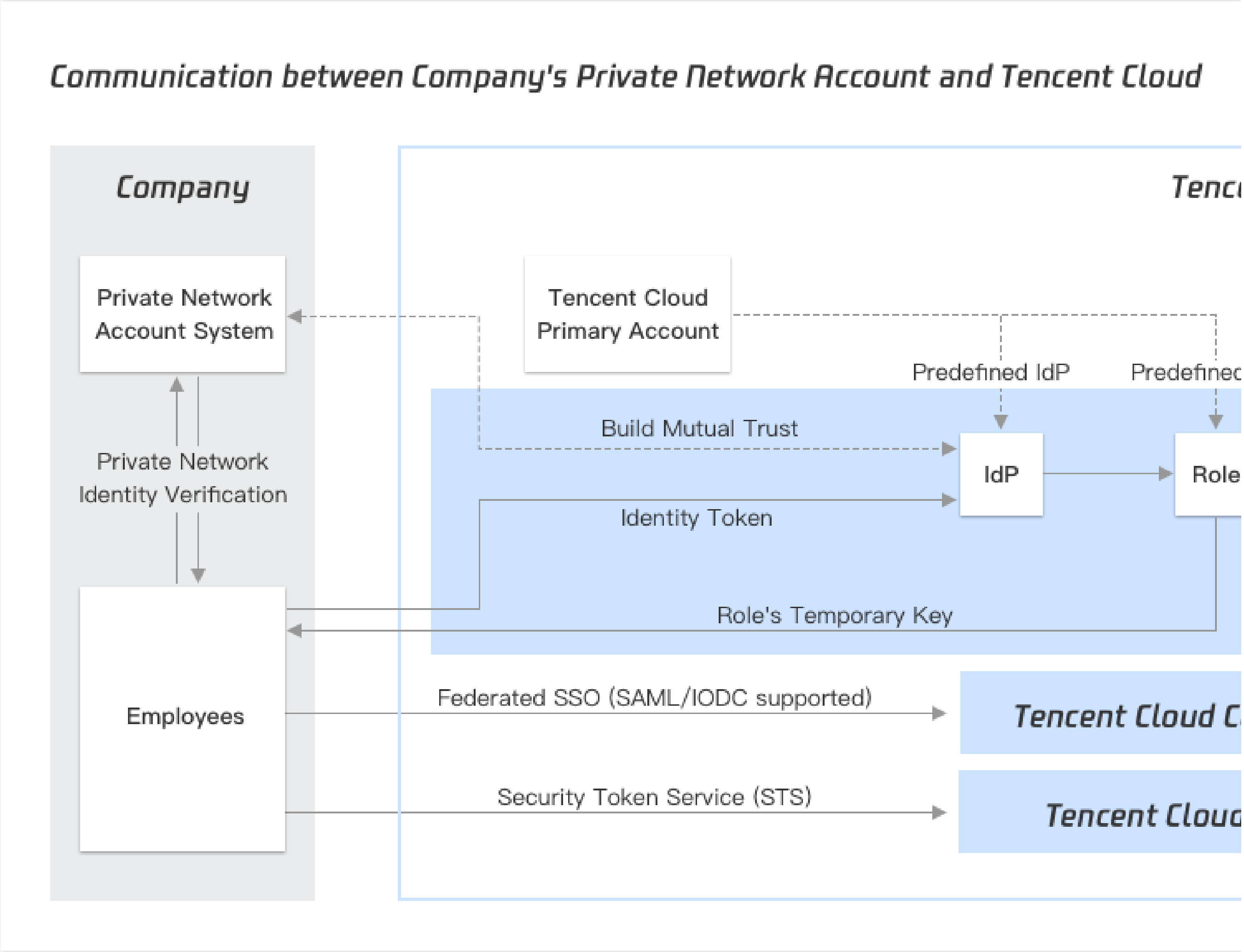
Tencent Cloud supports identity federation based on SAML 2.0 (Security Assertion Markup Language 2.0). SAML 2.0 is an open standard used by many identity providers (IdPs). IdP enables federated single sign-on (SSO), so you can authorize users that have been successfully authenticated to log in to the Tencent Cloud console or call the Tencent Cloud APIs without creating a CAM sub-user account for each of your members. In addition, as an open protocol, SAML 2.0 allows you use the proxy code directly instead of writing one by yourself, which has simplified federated authentication in Tencent Cloud.

SAML IdP

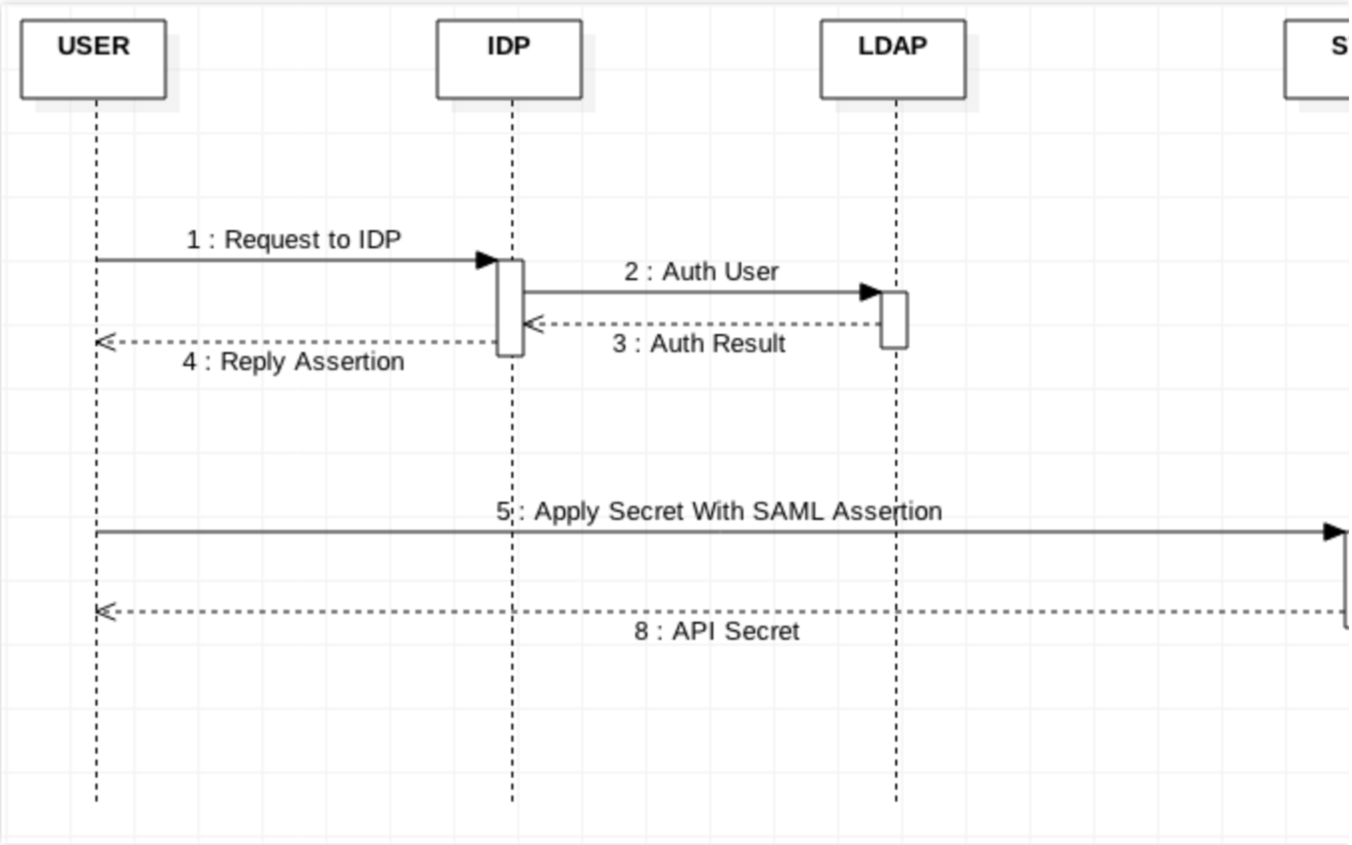
IdP is an entity in CAM, which can be deemed as a collection of external trusted accounts. SAML 2.0-based identity providers are the SAML 2.0-compliant IdPs. If you want to build trust between SAML 2.0 protocol-compatible IdPs (such as Microsoft Active Directory Federation Service) and Tencent Cloud for your enterprise or organization members to access Tencent Cloud resources, you need to create SAML IdPs. For more information, see Creating an IdP.

IdP Role

After creating an SAML IdP, you must create one or more IdP roles with the SAML IdP as the role entity. A role is a virtual identity with a group of permissions, and uses temporary security credentials to access resources. In the context of SAML 2.0 assertions, a role can be assigned to a federated user authenticated by an IdP. This role allows the IdP to request for temporary security credentials to access the Tencent Cloud resources. The policy associated with the role determines the scope of Tencent Cloud resources that can be accessed by the federated user. For more information on how to create SAML 2.0-based federated IdP roles, see Creating a Role.

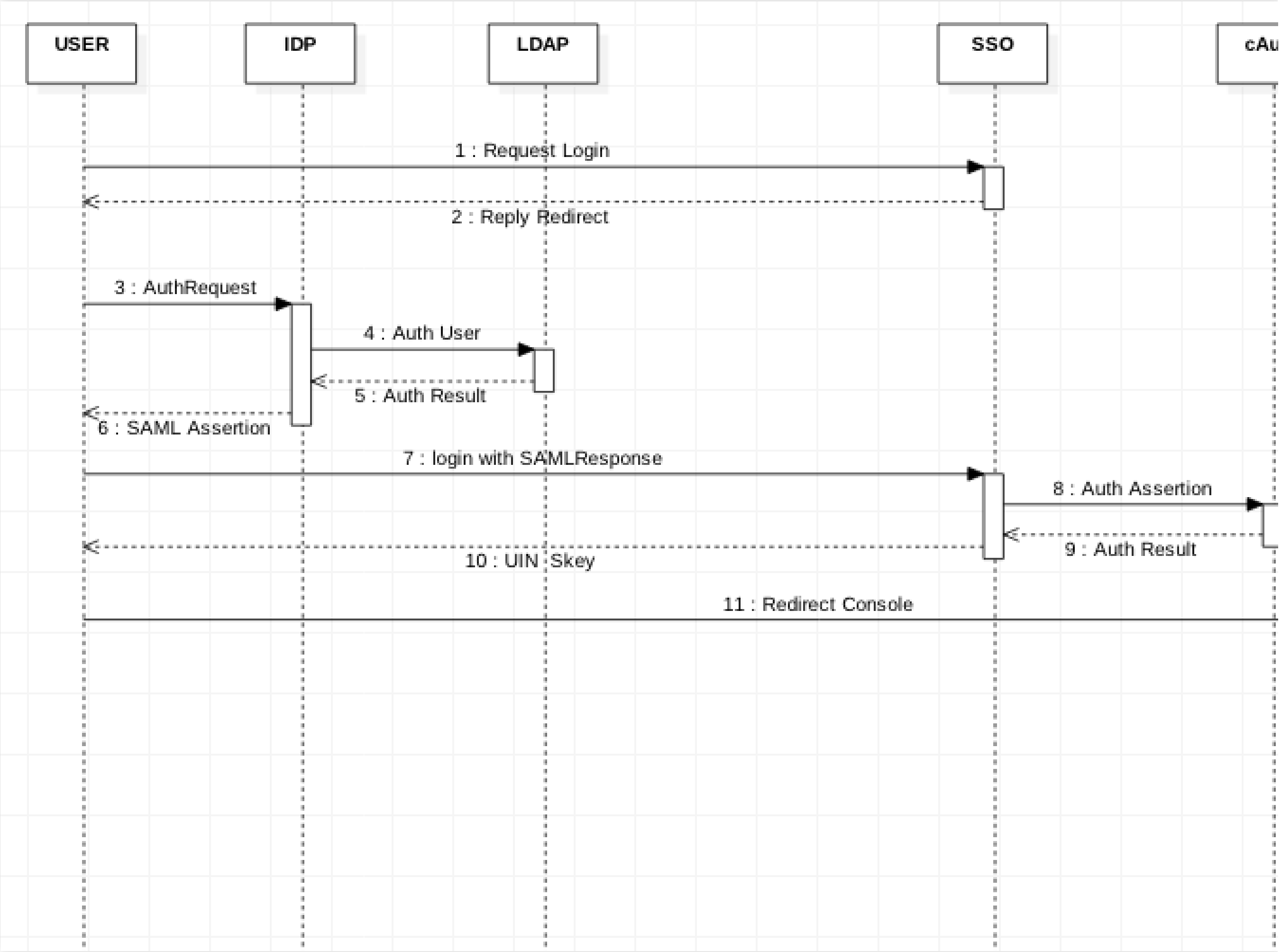

Communication between Company's Private Network Account and Tencent Cloud
Company
Private Network Account System
Private Network Identity Verification
Employees
Tenc
Tencent Cloud Primary Account
Predefined IdP
Predefined
Build Mutual Trust
IdP
Role
Identity Token
Role's Temporary Key
Federated SSO (SAML/IODC supported)
Tencent Cloud C
Security Token Service (STS)
Tencent Cloud

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. Return user authentication result
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 app requests sts:AssumeRoleWithSAML a temporary security key based on the SAML 2.0 assertion document, the resource description of the IdP and IdP role.
6. The SAML 2.0 assertion is authenticated by STS.
7. Return user authentication result.
8. The API applies for and returns a temporary credential to the client.

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



1. A user in your enterprise or organization uses a browser to access a Tencent Cloud service.
2. The Tencent Cloud service returns an authentication request to the browser.
3. The browser redirects the authentication request to the IdP of your enterprise or organization.
4. Your enterprise authenticates the user.
5. After the user is authenticated successfully, the user information will be returned to the IdP.
6. The IdP generates a standard SAML 2.0 assertion and returns it to the browser.
7. The browser redirects the SAML 2.0 assertion to Tencent Cloud.
8. Start the Tencent Cloud SSO login, request cAuth and verify the user's identity.
9. Return to Tencent Cloud verification results.
10. The verification is successful and the login status is returned.
11. Redirect to the Tencent Cloud Console.

Accessing Tencent Cloud Console as SAML 2.0 Federated Users

Last updated：2024-01-23 17:46:25

Overview

Tencent Cloud supports identity federation with SAML 2.0 (Security Assertion Markup Language 2.0). SAML 2.0 is an open standard used by many identity providers (IdPs). You can use SAML 2.0-based federation to integrate IdPs with Tencent Cloud. Federated single sign-on (SSO) can be implemented by using an IdP, and admins can authorize users that have their federated identity authenticated to log in to the Tencent Cloud console to manage Tencent Cloud resources, eliminating the need to create a CAM sub-user for each employee of the organization.

Directions

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. After verification, the portal will generate an SAML 2.0 identity verification response, which contains the assertions that identify the user's identity along with the related user attributes. The portal website will send the response to the client 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 identity verification response includes attributes mapping to multiple CAM roles, the system will first prompt the user to select the role they want to use to access the console.

From the user's perspective, the entire process is streamlined: the user starts the operation on the internal portal of your organization and finishes the operation in the Tencent Cloud console. There is no need to provide any Tencent Cloud credentials. For links to SSO configuration guides, please see the section below.

Configuring SAML 2.0-based IdP in organization

You can configure the identity store (such as Azure Active Directory) of your organization to use SAML 2.0-based IdPs like Azure Active Directory, OneLogin, and Okta. By using IdPs, you can generate a metadata document, which will describe your organization as an IdP with an identity verification key and will configure the portal of your organization to route user requests to access the Tencent Cloud console to the Tencent Cloud endpoint node, facilitating the use of SAML 2.0 assertions to perform identity verification. The configuration of the `metadata.xml` file generated by your IdP is subject to your IdP. For more information, please see the documentation of your IdP or read the following documents.

Azure Active Directory Single Sign-On to Tencent Cloud

OneLogin Single Sign-On to Tencent Cloud

Okta Single Sign-On to Tencent Cloud

Creating SAML IdP in CAM

You can create an SAML (Security Assertion Markup Language) 2.0 IdP in the CAM console. An IdP is an entity in CAM, which can be seen as a collection of external trusted accounts. An SAML 2.0-based federation IdP describes the IdP services supporting SAML 2.0. During creation, you can upload the IdP metadata document as described in Configuring SAML 2.0-based IdP in organization. For more information, please see Creating IdP.

Configuring permissions in Tencent Cloud for SAML provider user

You can create a role for building the trust between the IdP in your organization and Tencent Cloud. In the context of SAML 2.0 assertions, the role can be assigned to federated users that have been verified by the IdP. This role permits the IdP to request temporary security credentials to access Tencent Cloud resources. In this process, you can associate policies and configure use conditions for the role to determine the access scope and use conditions for federated users in Tencent Cloud. For more information, please see Creating Role.

Configuring SSO for IdP

Download and save the Tencent Cloud federation metadata XML file at http://cloud.tencent.com/saml.xml. Map the attributes of the IdP in your organization to the Tencent Cloud attributes to build the trust between the IdP in your organization and Tencent Cloud. How you install this file is subject to your IdP. Some providers offer an option for you to simply enter the URL, upon which they will get and install the file for you, while other providers require that you download the file and then upload it locally. For more information, please see the instructions from your IdP or the following documents:

Azure Active Directory Single Sign-On to Tencent Cloud

OneLogin Single Sign-On to Tencent Cloud

Okta Single Sign-On to Tencent Cloud

Sample SAML response

Below is an SAML sample:

©2013-2022 Tencent Cloud. All rights reserved.

```
<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/RoleSes
                    ...
                </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 whose `Name` attribute value is `https://cloud.tencent.com/SAML/Attributes/Role` . This element is required, and there can be multiple instances of it. The value of `AttributeValue` contained in it represents the role that the current user is allowed to play. The format of the value is a combination of role description and IdP description separated by comma (,).

Note:

If there are multiple roles, when you log in to the console, all roles will be listed on the page for you to choose.

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/{Acc
  <AttributeValue>qcs::cam::uin/{AccountID}:roleName/{RoleName2},qcs::cam::uin/{Acc
</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/{Accou
</Attribute>
```

Note:

Replace `{AccountID}` , `{RoleName}` , and `{ProviderName}` in the source `Role` attribute with the following:

Replace `{AccountID}` with your Tencent Cloud root account ID, which can be viewed on the Account Information page.

Replace `{RoleName}` with the role name you created for the IdP in Tencent Cloud (click here to see how to create a role for an IdP in Tencent Cloud), which can be viewed on the Roles page.
Replace `{ProviderName}` with the name of the SAML IdP you created in Tencent Cloud, which can be viewed on the Identity Providers page.
2. The `Attribute` element whose `Name` attribute value is `https://cloud.tencent.com/SAML/Attributes/RoleSessionName` . This element is required, and there can be only one instance of it. It is user-defined and can contain up to 32 characters. Below is a sample `Attribute` element of `RoleSessionName` , where `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：2024-01-23 17:46:25

Creating a SAML IdP

You can create an IdP via either Cloud Access Management Console or CAM API.

Creating an IdP 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 cannot exceed 40 KB. 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 **Create Provider**.

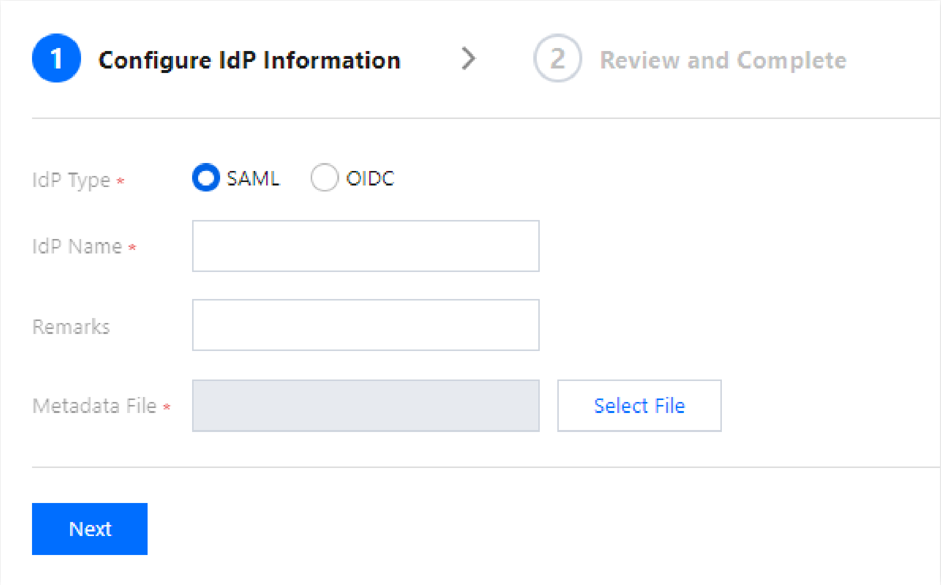
3. On the Create Identity Provider page, select the provider type as SAML, configure the provider information, and click **Next**.

IdP Name: Enter the name of the IdP.

Remarks: Enter any notes or comments you have about the current IdP.

Metadata Document: 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 only after the content of the metadata document is verified as valid.

©2013-2022 Tencent Cloud. All rights reserved.



1 Configure IdP Information > 2 Review and Complete

IdP Type * ● SAML ○ OIDC

IdP Name *

Remarks

Metadata File * Select File

Next

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

Creating an IdP via API

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

Creating an OIDC Identity Provider

Last updated：2024-01-23 17:46:25

You can create an IdP via either Cloud Access Management Console or CAM API.

Creating an IdP 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 **Create Provider**.

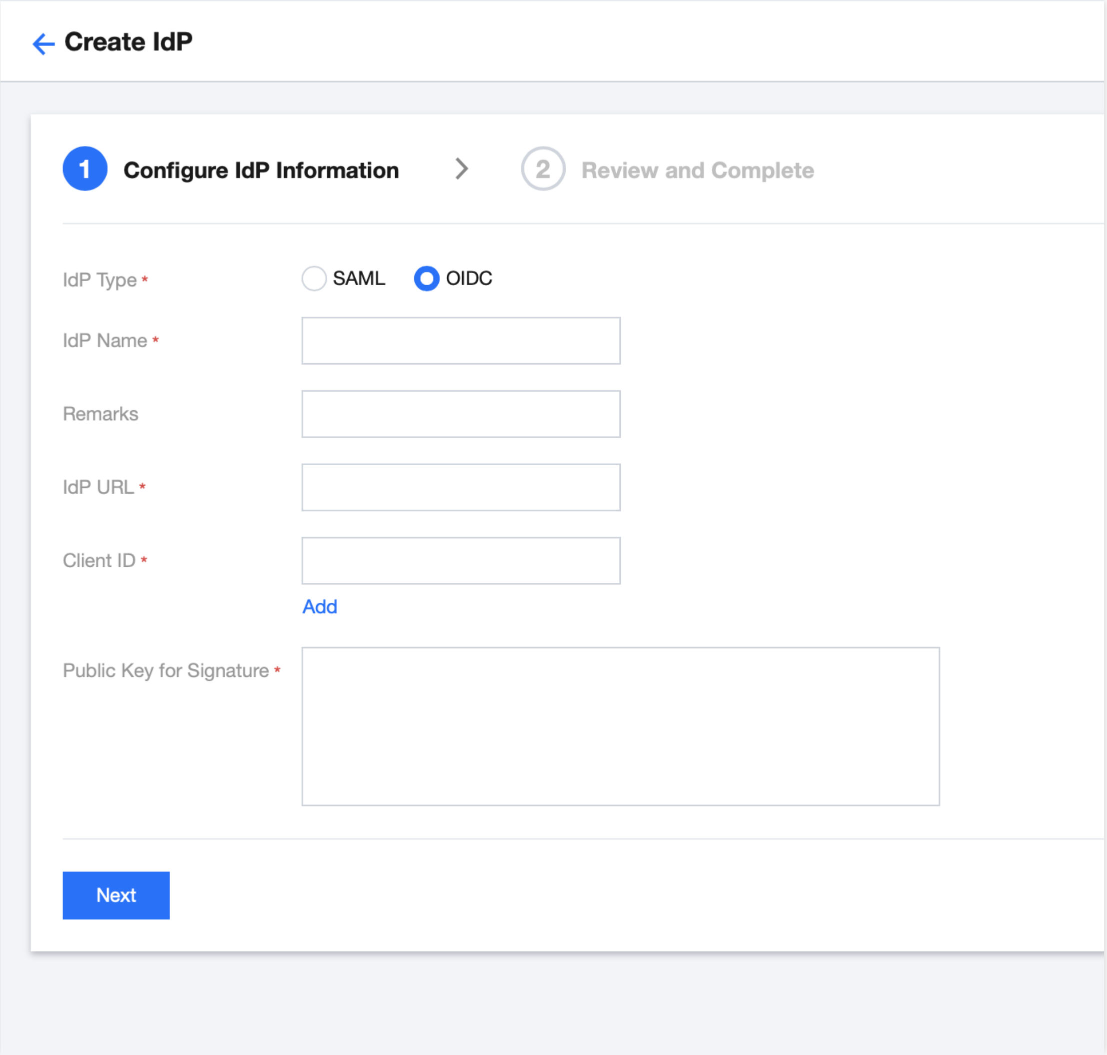
3. On the Create Identity Provider page, select the provider type as SAML, configure the provider information, and click **Next**.

IdP Name: Enter the name of the IdP.

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**.

Public Key for Signature: Public key used to verify the signature of the IdP's ID Token. It corresponds to the content (obtained by visiting the link) linked in the "jwks_uri" field in the OpenID Connect metadata document provided by the IdP. For the security of your account, it is recommended that you rotate the signature public key regularly.



Create IdP

1 Configure IdP Information > 2 Review and Complete

IdP Type * ○ SAML ● OIDC

IdP Name *

Remarks

IdP URL *

Client ID *

Public Key for Signature *

4. Click 'Next' to review the information about the IdP you entered. After confirming that everything is correct, click **Complete** to create the IdP.

Creating an IdP via API

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

Managing IdPs

Last updated：2024-01-23 17:46:25

Deleting SAML IdP

You can manage your IdPs via either CAM console or CAM API.

Deleting via console

1. Log in to the CAM console, and go to Identity Providers > Role-Based SSO.
2. Select the IdP you want to delete from the list and click **Delete** in the **Operation** column.
3. Confirm that you are deleting the right IdP, click **OK**.

Deleting via API

(Optional) To list all IdP information in pages, call ListSAMLProviders.

(Optional) To get the details of a specific IdP, call GetSAMLProvider.

To delete a SAML IdP, call DeleteSAMLProvider.

Modifying SAML IdP

You can modify an IdP via either CAM console or CAM API.

Modify via console

1. Log in to the CAM console, and go to Identity Providers > Role-Based SSO.
2. Select the IdP you want to modify from the list, and click the IdP name to enter the details page.
3. You can upload the metadata document to redefine the current IdP, or download the current metadata document.

Modifying via API

Update the description or the metadata document of an SAML IdP.

Call UpdateSAMLProvider

©2013-2022 Tencent Cloud. All rights reserved.

Azure Active Directory Single Sign-On

Last updated：2024-01-23 17:46:25

Introduction

Azure Active Directory (Azure AD) is a cloud-based identity and access management service released by Microsoft. It can be used to help employees manage internal and external resources. Tencent Cloud supports identity federation with SAML 2.0 (Security Assertion Markup Language 2.0). SAML 2.0 is an open standard used by many identity providers (IdPs). You can use the SAML 2.0-based identity federation to integrate Azure Active Directory with Tencent Cloud, implementing single sign-on through the Azure AD account to log in to the Tencent Cloud console and manage Tencent Cloud resources without requiring the creation of a CAM sub-user for each employee of the enterprise or organization.

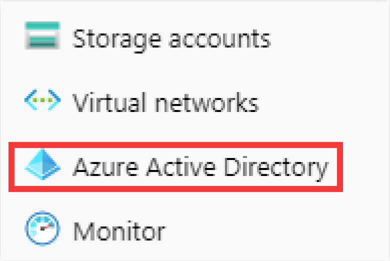
Directions

Creating Azure AD Enterprise Applications

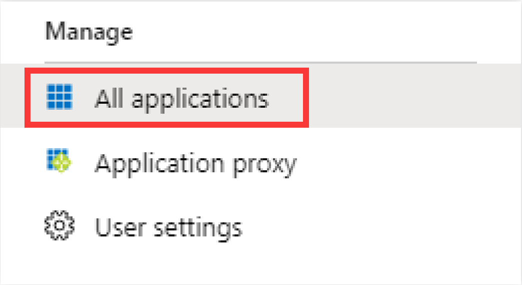
Note:

This step creates an Azure AD enterprise application. If you’re already using one, you can skip this step and go straight to configuring CAM.

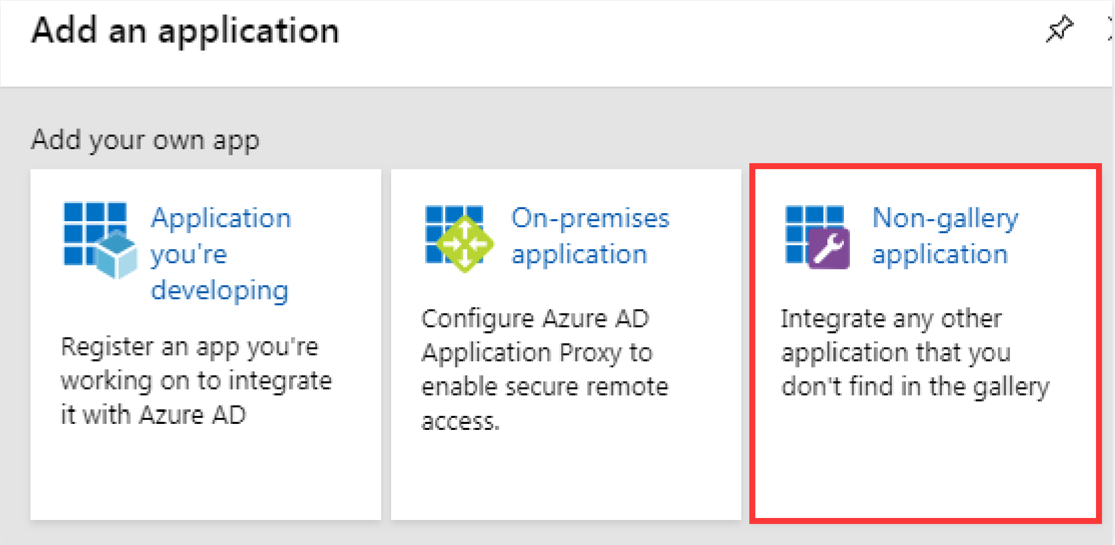
1. Go to the Azure AD Portal and click **Azure Active Directory** in the left sidebar. This is shown in the following figure:



2. Click **Enterprise Applications** and select **All Applications**. This is shown in the following figure:



3. Click **New Application** to open the **Add Application** window. Select **Non-gallery Application**. This is shown in the following figure:



Add an application

Add your own app

Application you're developing

Register an app you're working on to integrate it with Azure AD

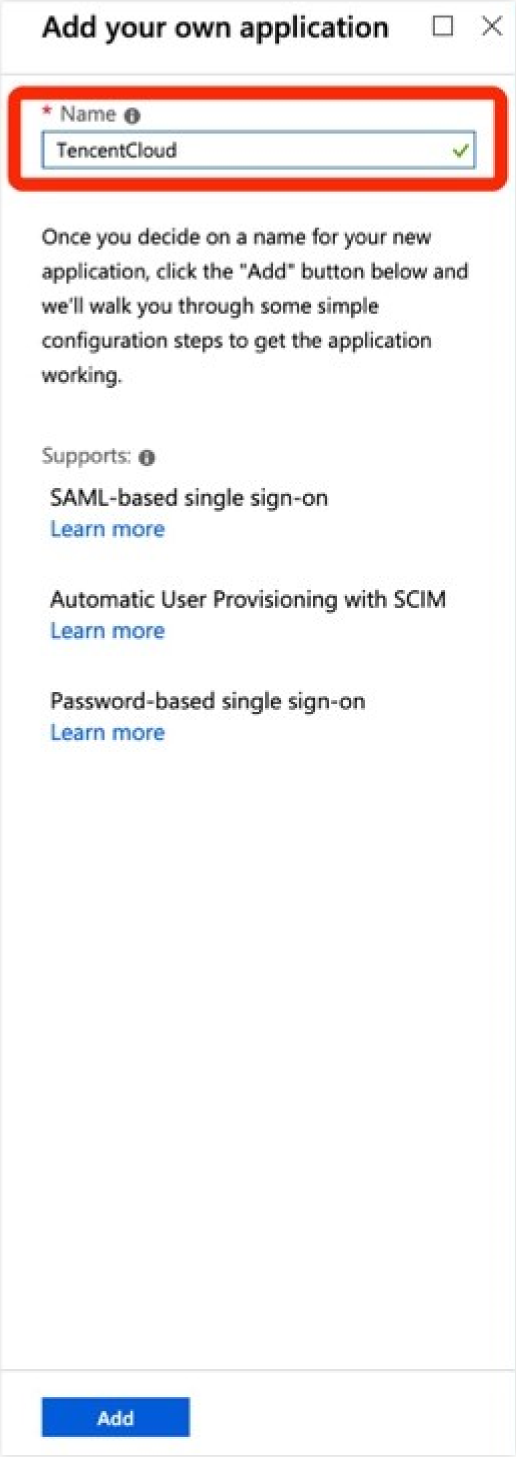
On-premises application

Configure Azure AD Application Proxy to enable secure remote access.

Non-gallery application

Integrate any other application that you don't find in the gallery

4. Enter **Name** and click **Add** to complete the creation of the Azure AD application. This is shown in the following figure:



Add your own application

* Name

TencentCloud

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports:

SAML-based single sign-on
Learn more

Automatic User Provisioning with SCIM
Learn more

Password-based single sign-on
Learn more

Add

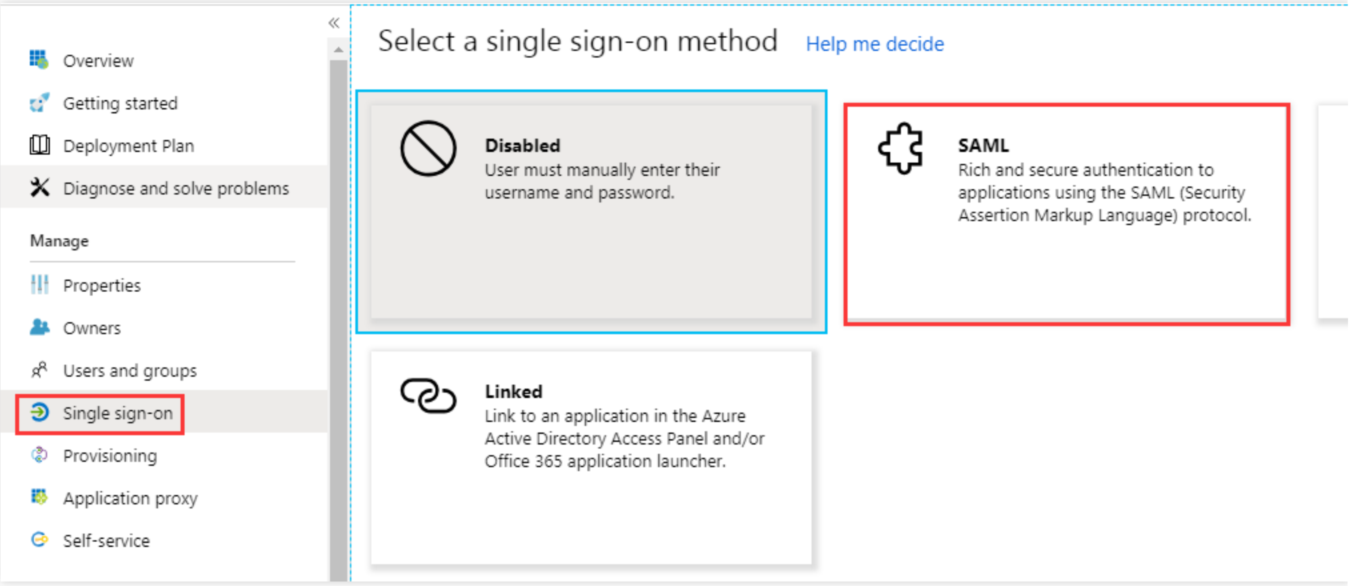
Configuring CAM

Note:

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

1. In the left sidebar, go to **Azure Active Directory** > **Enterprise Applications**, and select 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 **Select a Single Sign-On Method** page, select **SAML**. This is shown in the following figure:



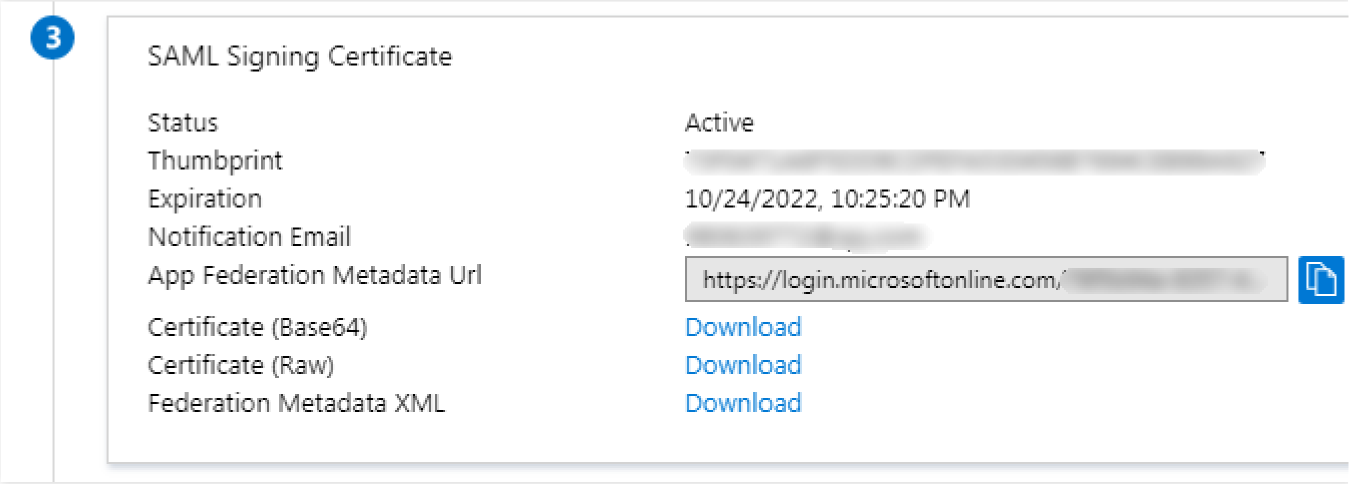
Select a single sign-on method

Disabled
User must manually enter their username and password.

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

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

4. In the **SAML Single Sign-On** preview page, download the **Federation Metadata XML** file under **SAML Signing Certificate**. This is shown in the following figure:



SAML Signing Certificate

Status	Active
Thumbprint	[redacted]
Expiration	10/24/2022, 10:25:20 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

5. Create the SAML identity provider and roles in Tencent Cloud. For more information, see Creating an IdP.

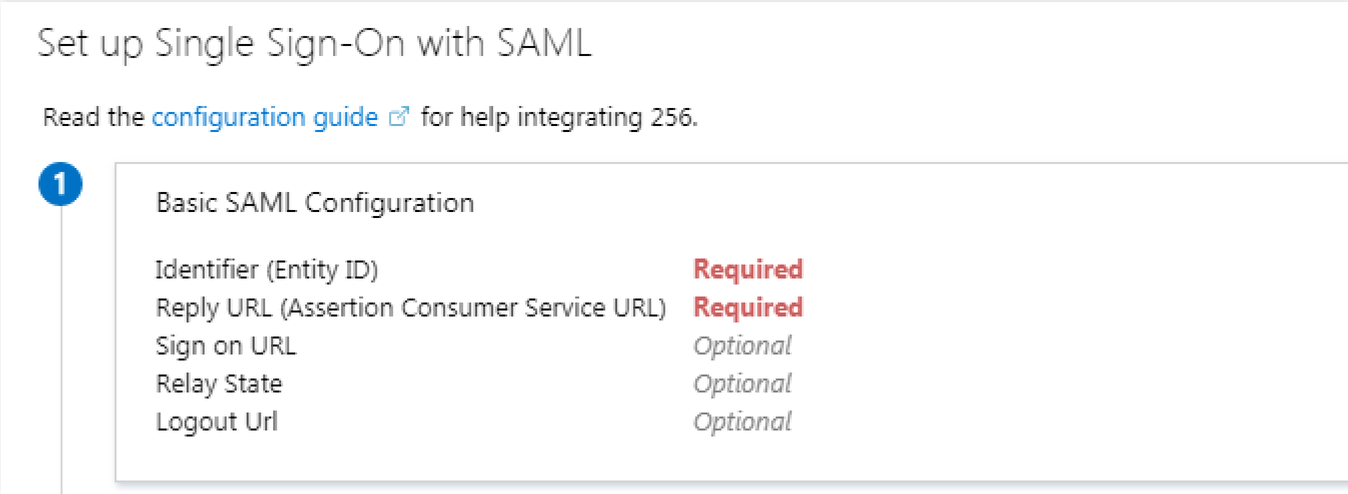
Configuring the Azure AD Single Sign-On

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 upper right of **Basic SAML Configuration**. This is shown in the following figure:



Set up Single Sign-On with SAML

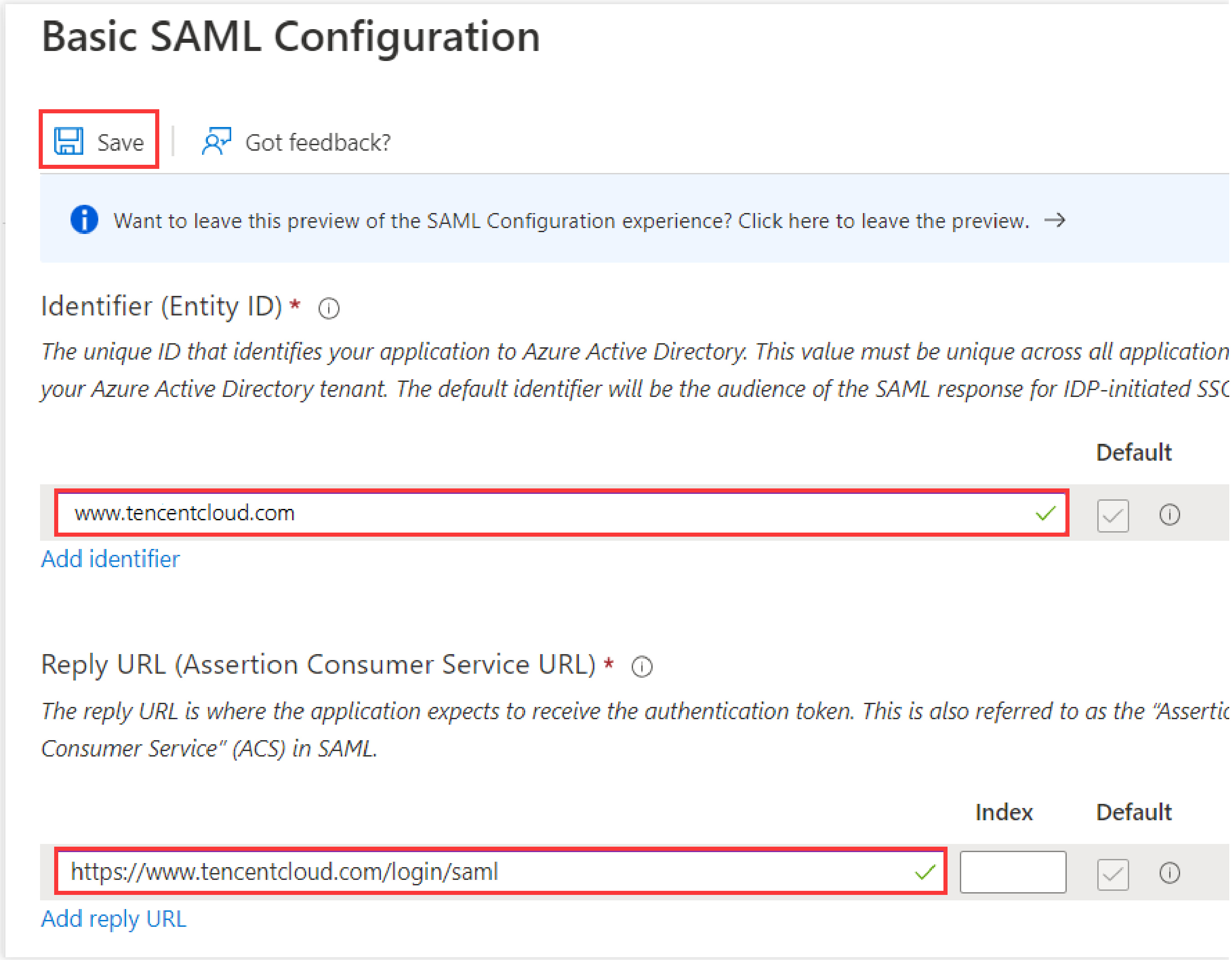
Read the configuration guide for help integrating 256.

1

Basic SAML Configuration

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

2. In the **Basic SAML Configuration** editing page, enter the following information and click **Save**. This is shown in the following figure:



Basic SAML Configuration

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) *

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

	Default
www.tencentcloud.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 "Assertic Consumer Service" (ACS) in SAML.

	Index	Default
https://www.tencentcloud.com/login/saml ✓		☑

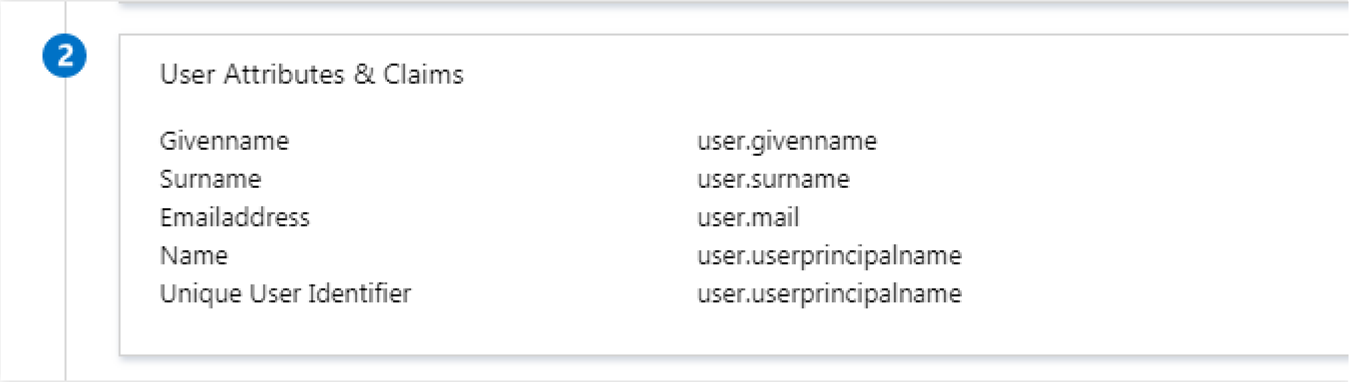
You can configure it according to the site where your Tencent Cloud account is located

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

3. In the **SAML Single Sign-On** overview interface, click

✎

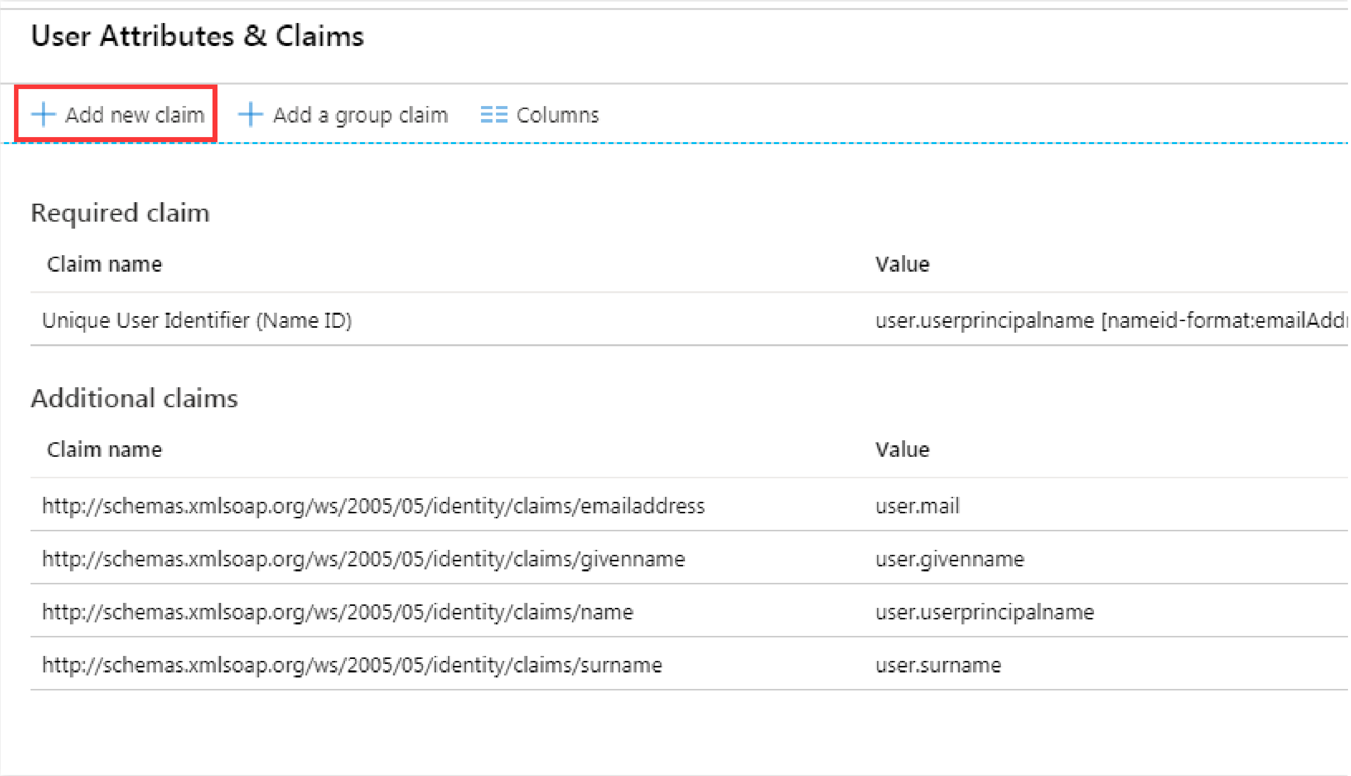
in the upper right corner of **User Attributes and Claims** to open the **User Attributes and Claims editor. This is shown in the following figure:



User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

4. In the **User Attributes and Claims** editing page, click **Add New Claim** to go to the **Manage User Claims** page. This is shown in the following figure:



Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddr

Additional claims

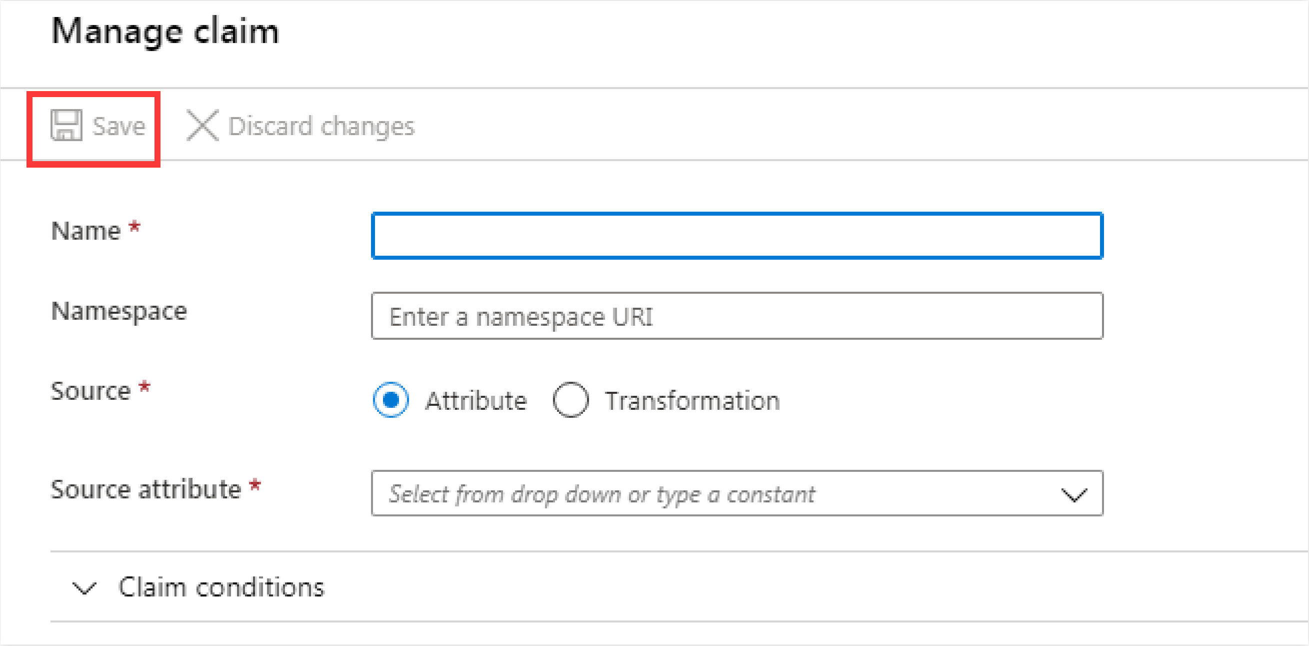
Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

5. In the **Manage User Claims** page, add the following two claims, and click **Save**. This is shown in the following figure:

Name	Namespace	Source	Source attribute
Role	https://cloud.tencent.com/SAML/Attributes	Attribute	qcs::cam::uin/{AccountID}:roleNa provider/{ProviderName}
RoleSessionName	https://cloud.tencent.com/SAML/Attributes	Attribute	Azure

Note:

Replace {AccountID}, {RoleName}, and {ProviderName} of the **Role** source attribute with the following content:
{AccountID}: Replace this with your Tencent Cloud account ID. You can view this at Account Information - Console.
{RoleName}: Replace this with the role name you have created in Tencent Cloud for the identity provider. For more information, see Creating a Role. Role names can be viewed in Role - Console. If you need to add more, you can add them in this format: qcs::cam::uin/{AccountID}:roleName/{RoleName}. Separate them using semicolons (;).
{ProviderName}: Replace this with the SAML identity provider name that you created on Tencent Cloud. You can view this at Identity Providers - Console.

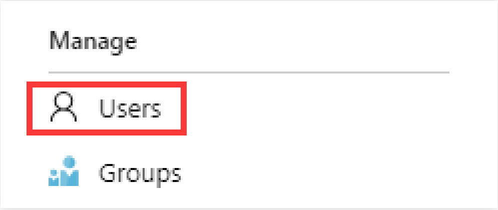


Configuring Azure AD Users

Note:

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

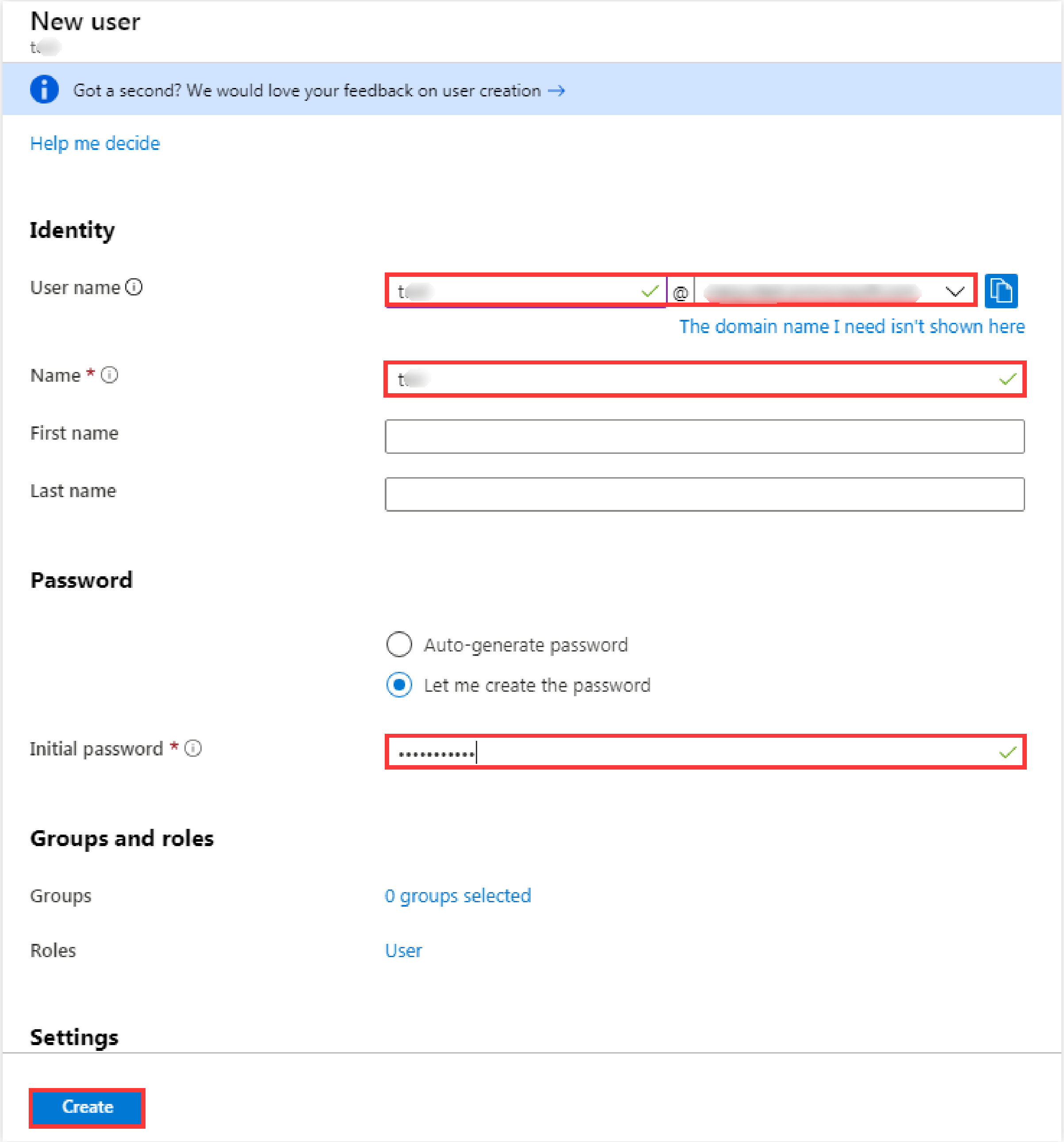
1. Click Azure Active Directory in the left sidebar. Click User to open All Users. This is shown in the following figure:



2. Click

New u

ser in the upper left corner. In the **User** page, enter **Name**, **User name**, and select**Show Password** to verify the password. Once the information is correct, click **Create** on the lower center to complete creation. This is shown in the following figure:



New user

t[redacted]

Got a second? We would love your feedback on user creation →

Help me decide

Identity

User name ⓘ: t[redacted] ✓ @ [redacted]

The domain name I need isn't shown here

Name * ⓘ: t[redacted] ✓

First name:

Last name:

Password

○ Auto-generate password

● Let me create the password

Initial password * ⓘ: ••••••••••• ✓

Groups and roles

Groups: 0 groups selected

Roles: User

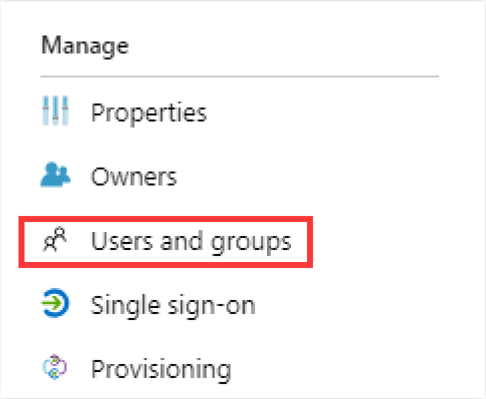
Settings

Create

Note:

The username format is as follows: Username@domain name. Usernames can be customized. Click **Azure Active Directory** in the left sidebar to open the overview page. You can view previously configured **Initial Domain Name** here. You can copy and save the username and password for future use.

3. In the left sidebar, go to **Azure Active Directory** > **Enterprise applications**, and select the application you created to go to the application overview page, and then click **Users and Groups**. This is shown in the following figure:



Manage

Properties

Owners

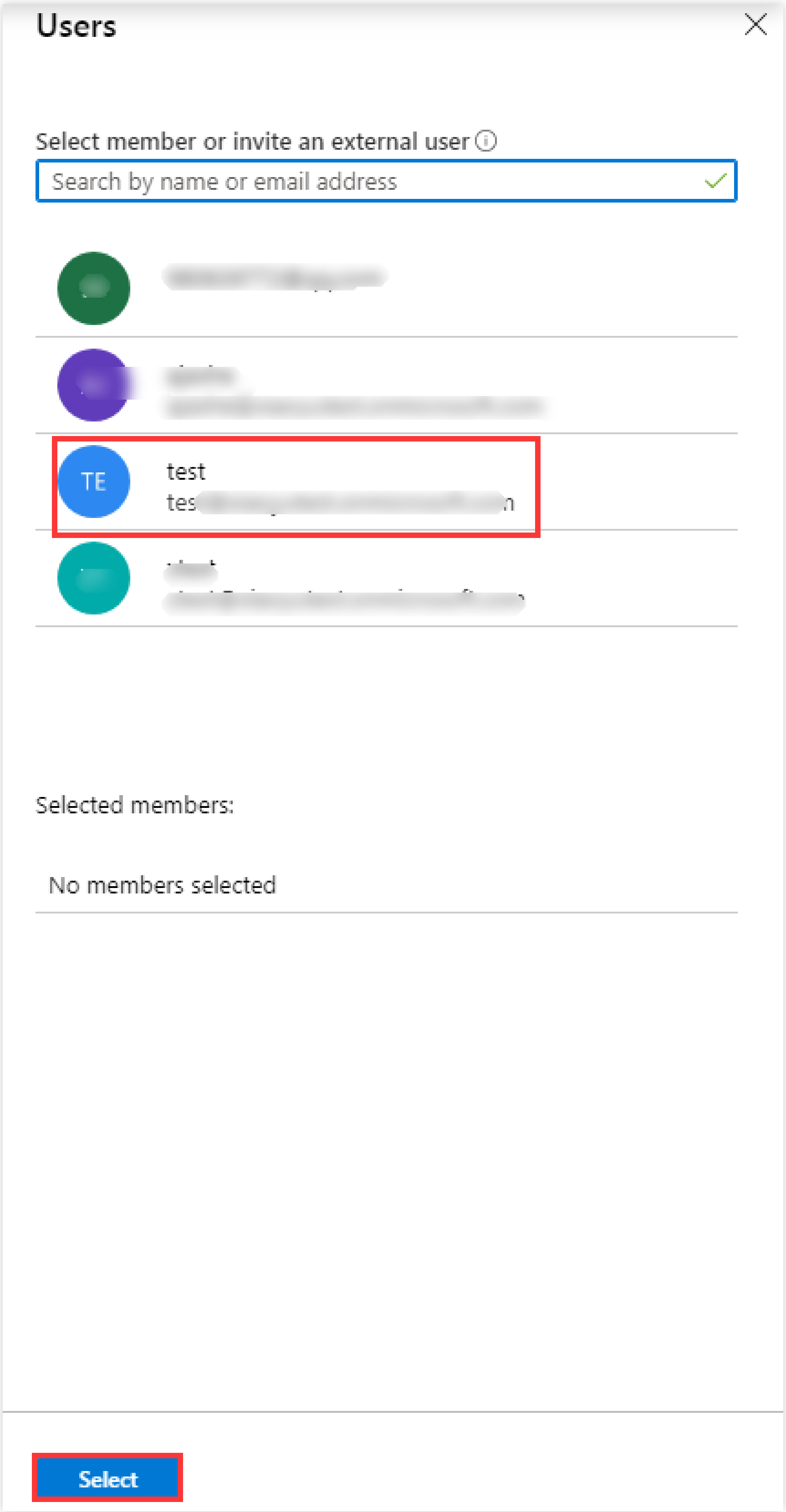
Users and groups

Single sign-on

Provisioning

4. Click **Add User** to open **Users and Groups**. Select the user you created in Step 2 and click the **Select** button. This is shown in the following figure:

©2013-2022 Tencent Cloud. All rights reserved.



Users

Select member or invite an external user ⓘ

Search by name or email address

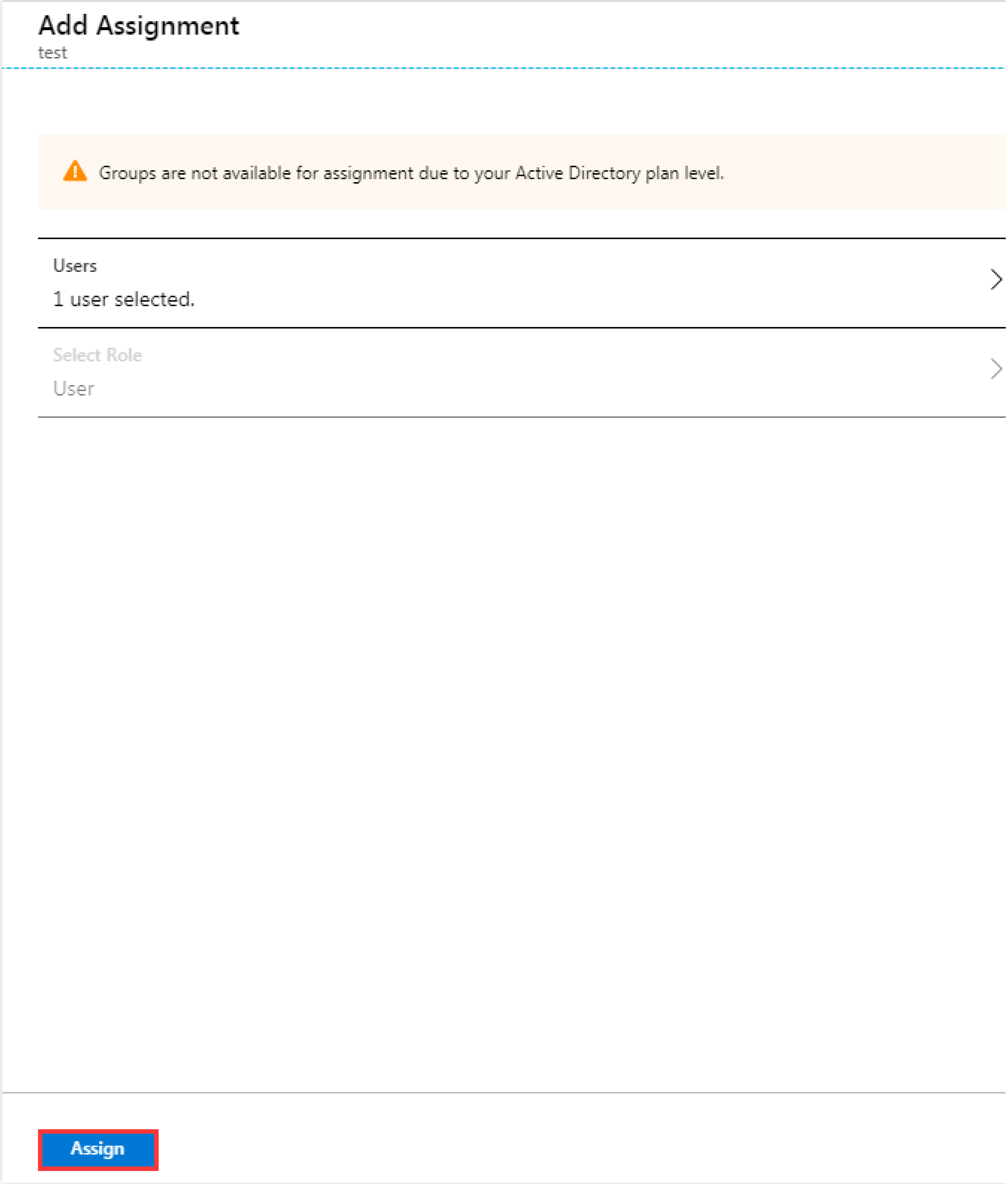
TE test

tes

Selected members:

No members selected

5. You will be redirected to the **Add Assignment** page. After confirming, click **Assign**. This is shown in the following figure:



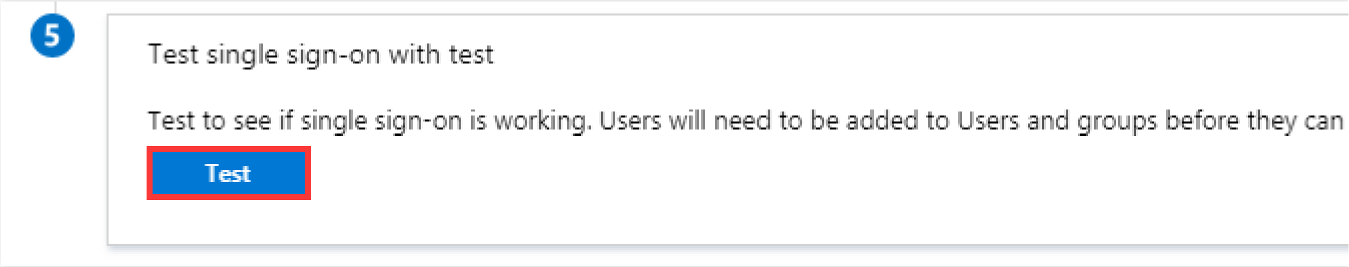
Add Assignment
test

⚠ Groups are not available for assignment due to your Active Directory plan level.

Users
1 user selected.

Select Role
User

6. In the left sidebar, go to **Azure Active Directory** > **Enterprise Applications**, and select the application you created to go to the application overview page.
7. Click **Single Sign-On** to open the **SAML Single Sign-On** overview page. Click **Test**. This is shown in the following figure:



5

Test single sign-on with test

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

8. In 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：2024-01-23 17:47:38

Overview

OneLogin is a cloud identity access management solution provider. You can log in to all the internal system platforms of your organization through OneLogin's identity verification system with one click. Tencent Cloud supports identity federation with Security Assertion Markup Language 2.0 (SAML 2.0). SAML 2.0 is an open standard used by many IdPs such as OneLogin.

Federated single sign-on (SSO) can be implemented by using an IdP, and admins can authorize users with their federated identity authenticated to log in to the Tencent Cloud console or call TencentCloud APIs, eliminating the need to create a CAM sub-user for each employee in the organization.

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

Directions

Creating a OneLogin enterprise application

Note:

This step creates a OneLogin enterprise application. If you are already using one, skip this step and go straight to CAM configuration.

This document uses the application name **test** as an example.

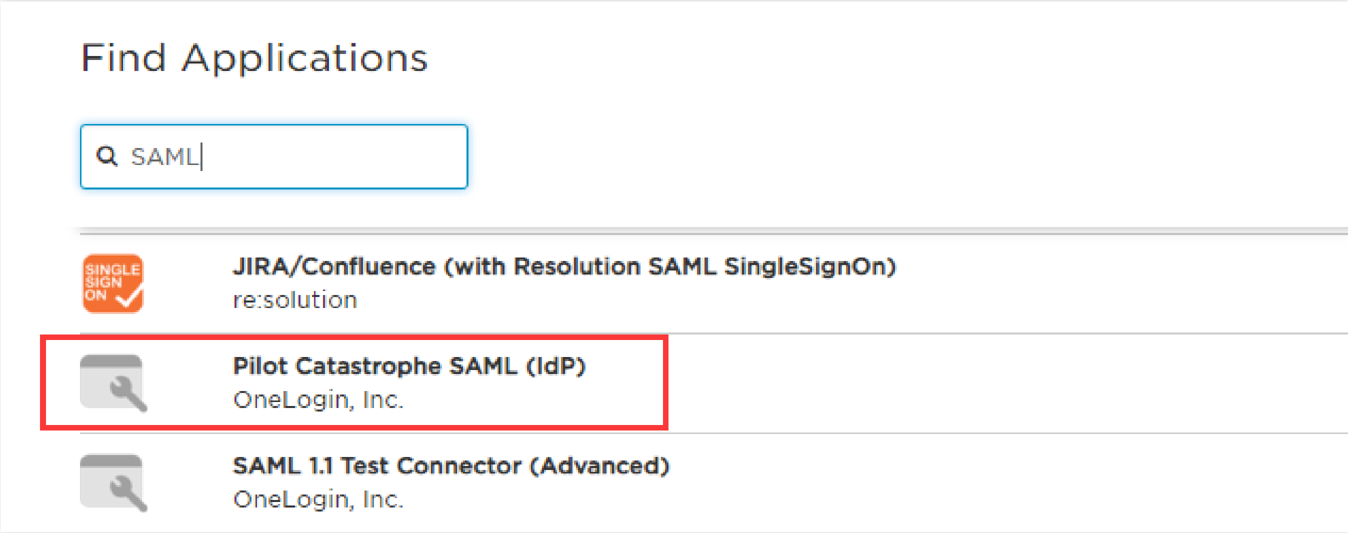
1. Log in to the OneLogin website and click **Applications** to enter the application managem

ent p

age.

2. On the application management page, click **Add App** in the top-right corner.

3. In the search box, enter **SAML** and press **Enter**. In the results list, click **Pilot Catastrophe SAML (IdP)** as shown below:



Find Applications

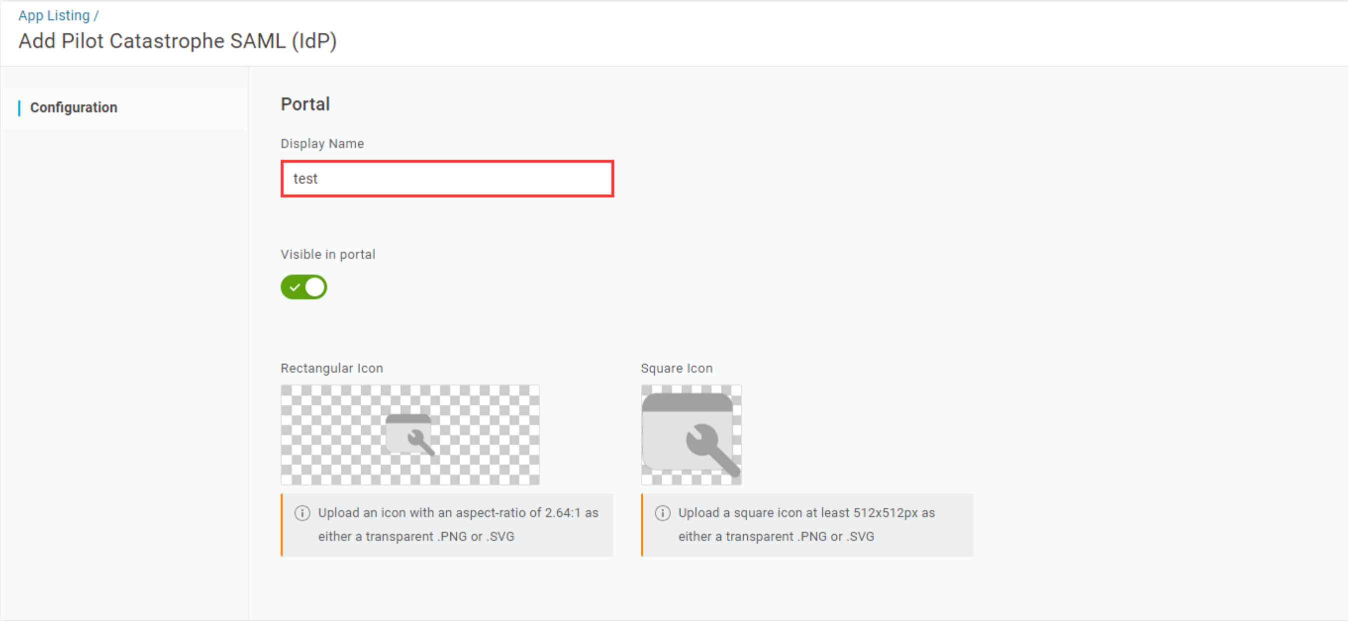
SAML

JIRA/Confluence (with Resolution SAML SingleSignOn)
re:solution

Pilot Catastrophe SAML (IdP)
OneLogin, Inc.

SAML 1.1 Test Connector (Advanced)
OneLogin, Inc.

4. In **Display Name** field, enter the application name. Click **Save** in the top-right corner to complete the application creation as shown below:



App Listing /
Add Pilot Catastrophe SAML (IdP)

Configuration

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

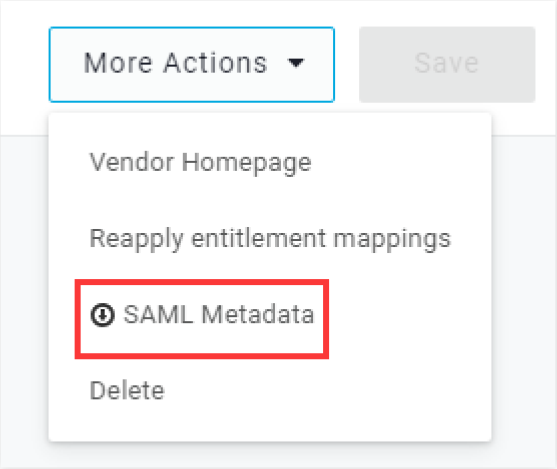
Note:

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 created application **test**.

2. Click **More Actions** in the top-right corner and select **SAML Metadata** to download the IdP cloud data file as shown below:



3. Create the Tencent Cloud CAM IdP and role. For detailed directions, see Creating an IdP and Creating Role.

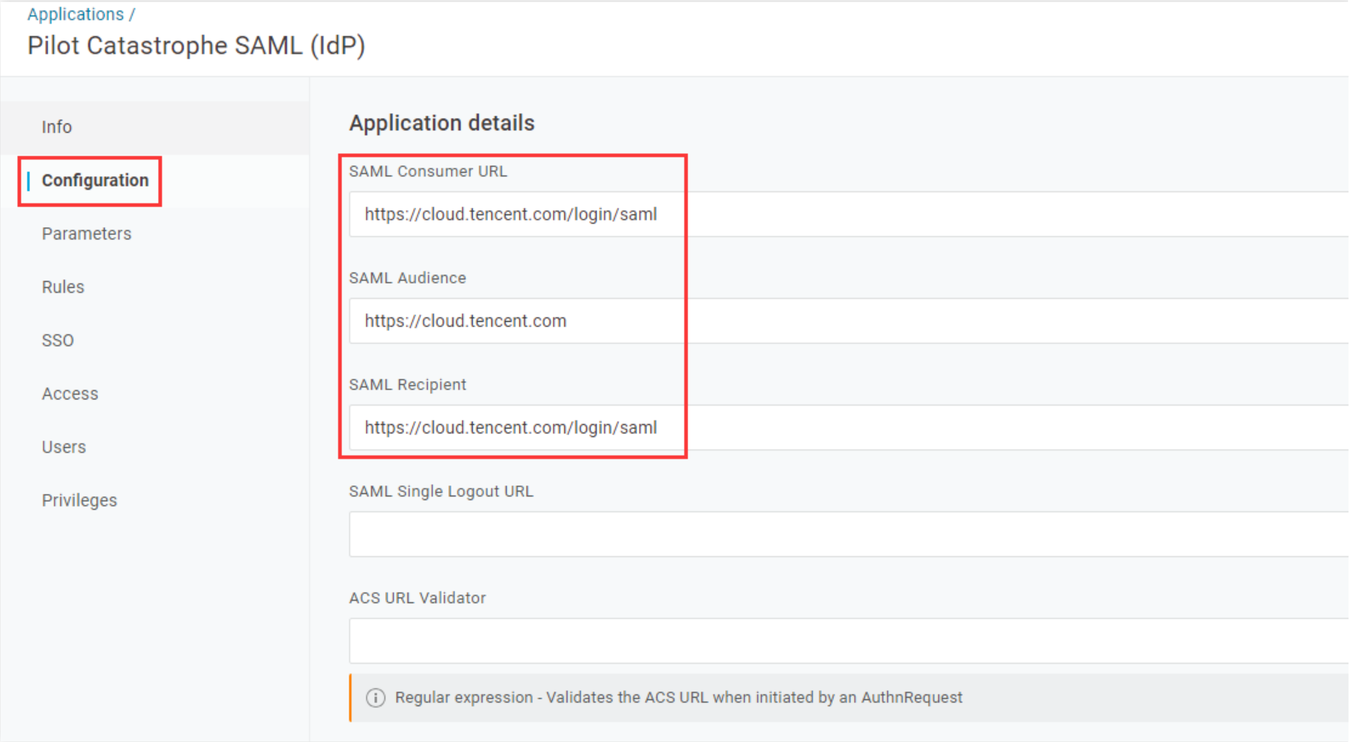
Configuring OneLogin SSO

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 the created **test** application to enter the application editing page.

2. Select the **Configuration** tab, enter the following content, and click **Save** as shown below:



Application details

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 F
Tencent Cloud International	https://www.tencentcloud.com/login/saml	https://www.tencentcloud.com/login/saml	https://v

3. Click **Parameters**, select **Add Parameter**, and add the following two items:

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

Note：

Replace {AccountID}, {RoleName}, and {ProviderName} of the **Role** source attribute with the following content:

{AccountID}: Replace this with your Tencent Cloud account ID. You can view this in Account Information in the console.

{RoleName}: Replace this with the role name you created on Tencent Cloud. You can view this in Role in the console.

{ProviderName}: Replace this with the SAML IdP name that you created on Tencent Cloud. You can view this in IdPs in the console.

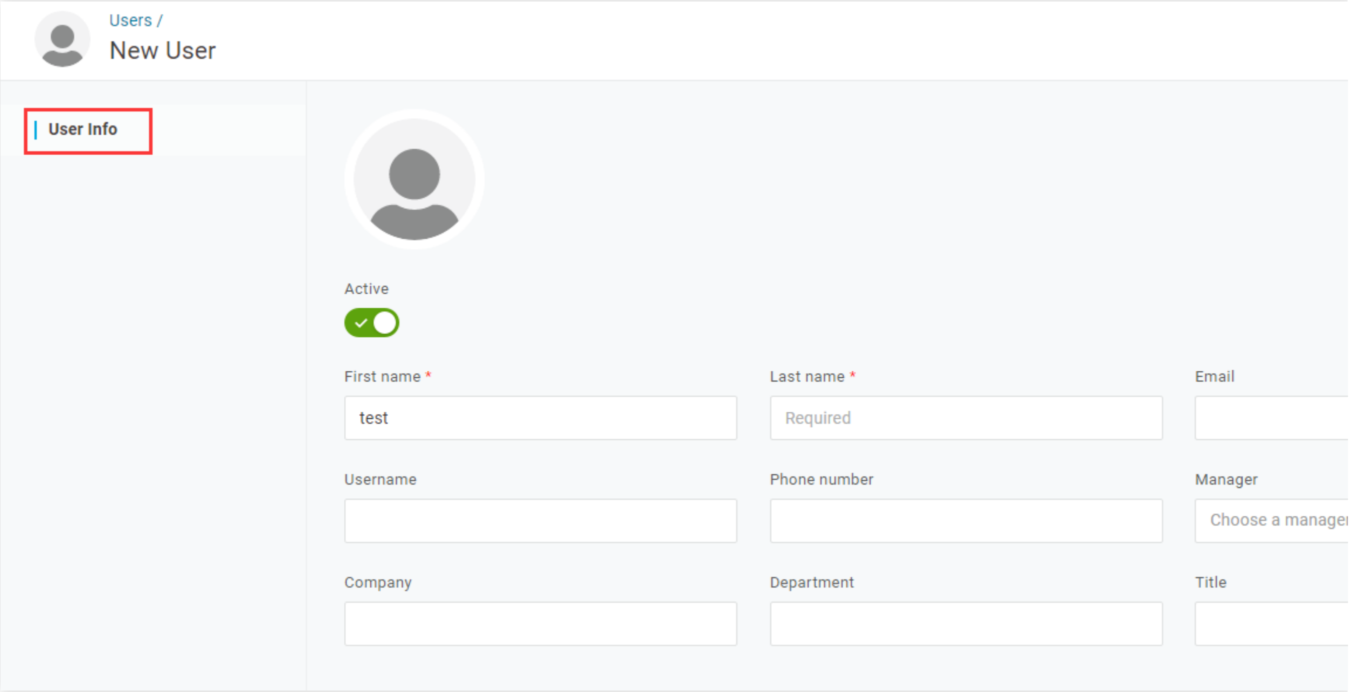
4. Click **Save** in the top-right corner to save the configuration.

Configuring a OneLogin user

1. Log in to the OneLogin website and click **Users** to enter the user management page.
2. Click **New User** in the top-right corner to enter the user creation page.
3. Enter **Fir**

st N

ame, **Last Name**, **Email**, and **Username** and click **Save User** as shown below:



Active

First name * test

Last name * Required

Email

Username

Phone number

Manager Choose a manage

Company

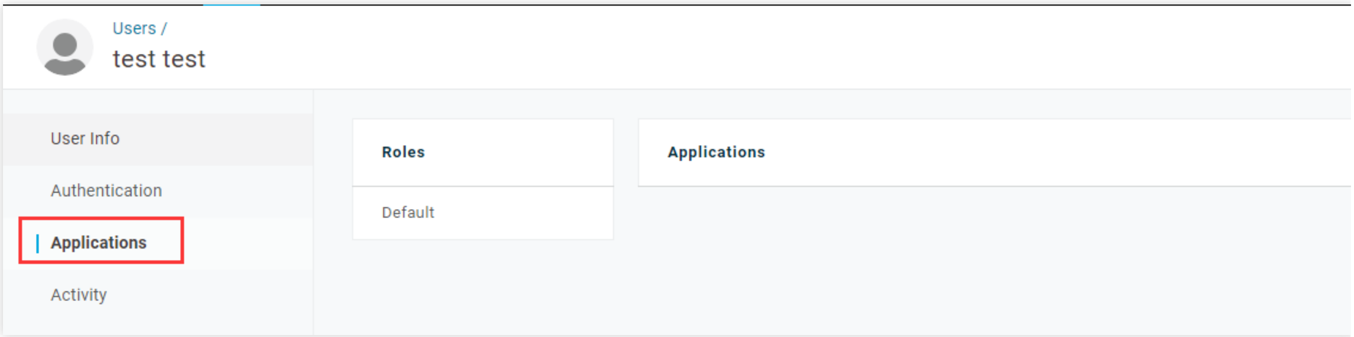
Department

Title

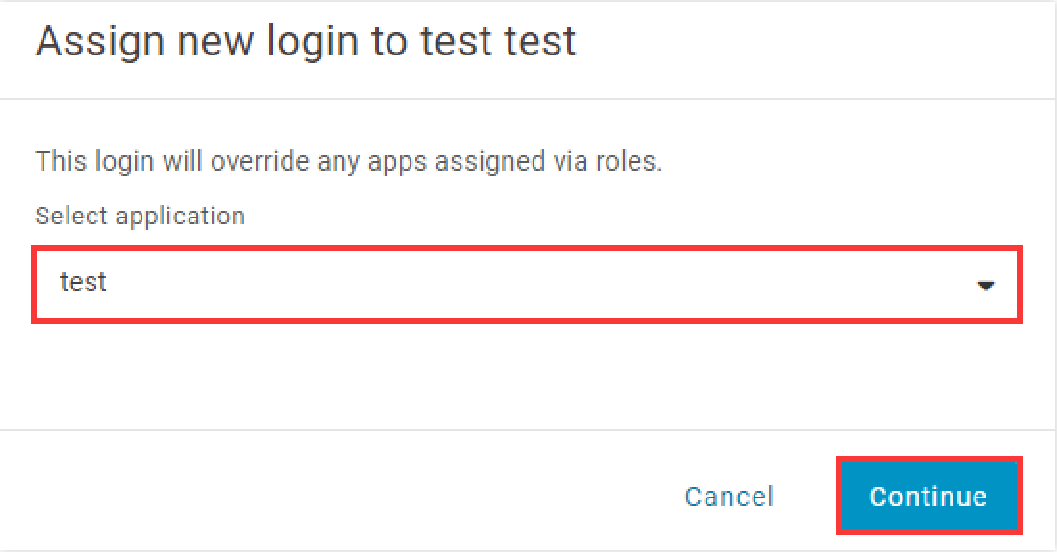
Note:

Check your email for the password of this account, or click **More Actions** and select **Change Password** to change the password.

4. Click **Applications** on the user editing page. Select + on the right as shown below:



5. In the pop-up window, select the SAML **test** application that you created. Click **Continue** as shown below:



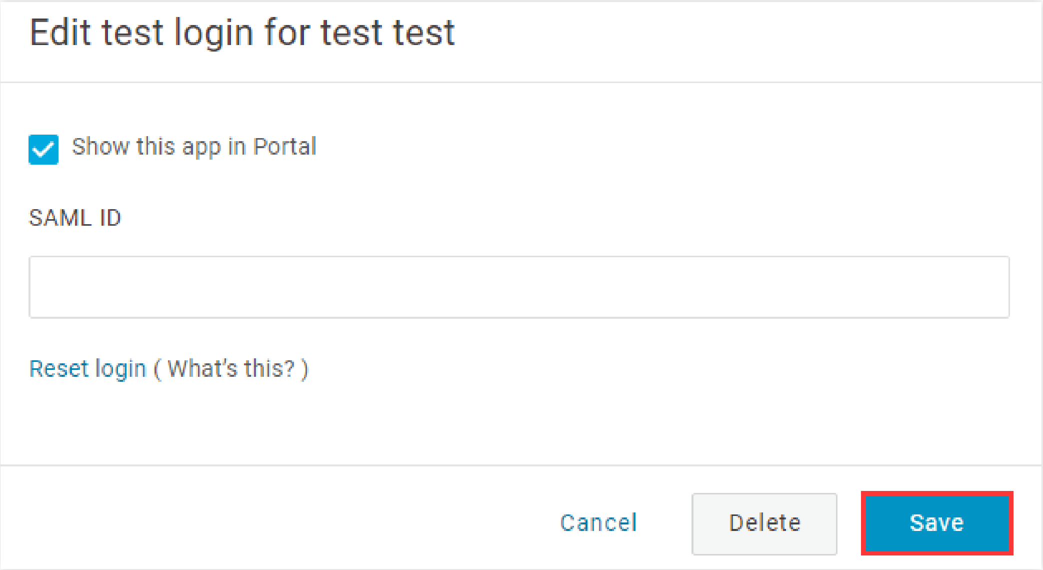
Assign new login to test test

This login will override any apps assigned via roles.

Select application

test

6. On the editing page, click **Save** as shown below:



Edit test login for test test

☑ Show this app in Portal

SAML ID

7. Use the account created in step 3 to log in to OneLogin, and access the SAML **test** application created in the preceding sections. You will be redirected to the Tencent Cloud console.

Okta Single Sign-On

Last updated：2024-01-23 17:46:25

Overview

Okta is a solution provider for identification and access management. Tencent Cloud supports identity federation with Security Assertion Markup Language 2.0 (SAML 2.0). SAML 2.0 is an open standard used by many identity providers (IdPs). SAML 2.0-based federation can be used to integrate Okta with Tencent Cloud. Then, federated single sign-on (SSO) can be implemented by using an Okta account, and admins can authorize users that have their federated identity authenticated to log in to the Tencent Cloud console for resource management, eliminating the need to create a CAM sub-user for each employee in the organization.

Directions

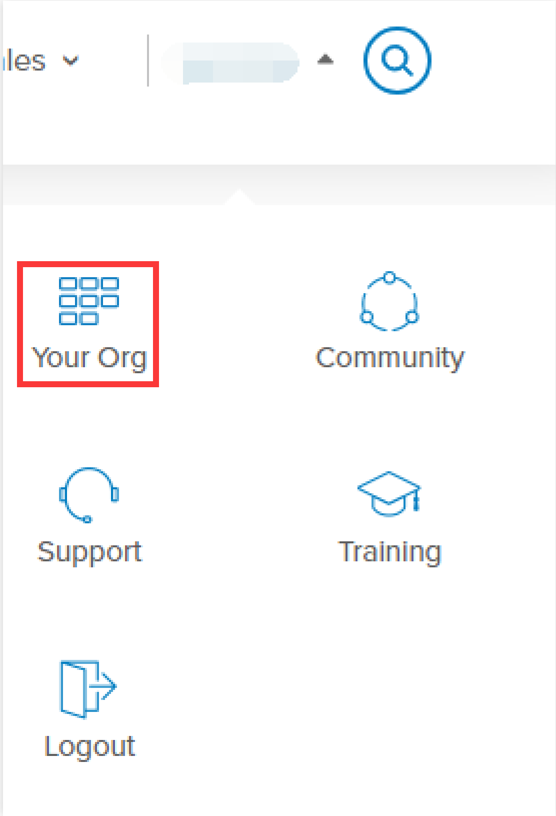
Creating an Okta application

Note:

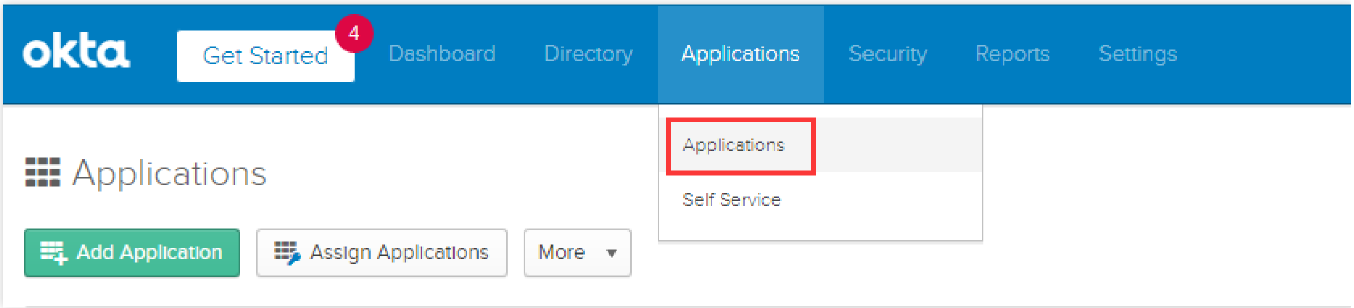
This step creates an Okta application. If you are already using one, skip this operation go straight to configuring CAM.

1. Log in to the Okta website, click your **username**, and select **Your Org** in the top-right corner as shown below:

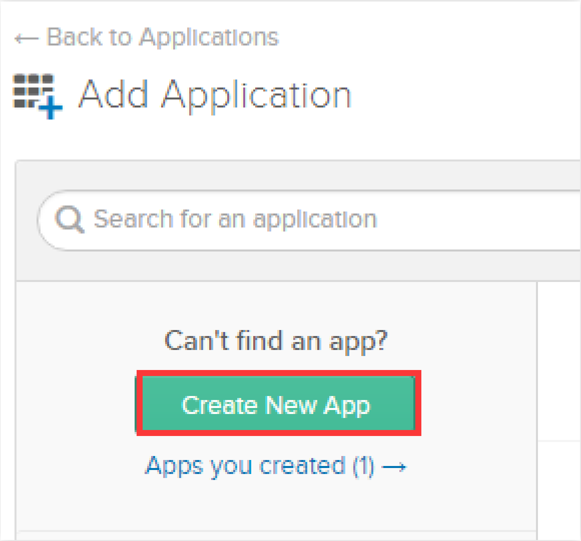
©2013-2022 Tencent Cloud. All rights reserved.



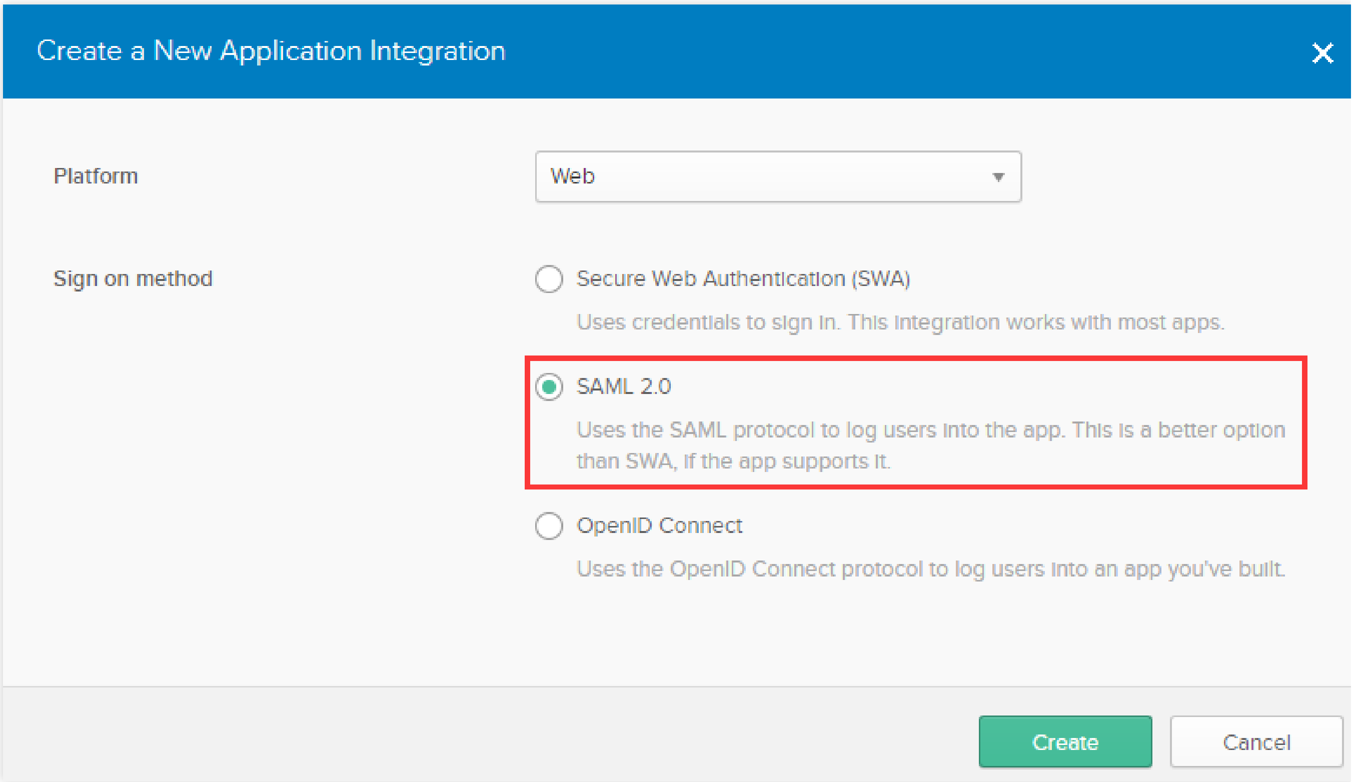
2. On the Okta homepage, click **Admin** in the top-right corner to enter
 the **Admi**
n page.
3. On the **Admin** page, select **Applications** to go to the application man
agemen
t page as shown below:



4. On the application management page, click **Add Application**.
5. On the **Add Application** page, click **Create New App** as shown below:



6. In the **Create a New Application Integration** pop-up window, select the platform, set the sign-on method to SAML 2.0, and click **Create** as shown below:


Create a New Application Integration

Platform: Web

Sign on method

○ Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.

● SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

○ OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

7. On the **General Settings** page, set **App name**, **App logo** (optional), and **App visibility** (optional) and click **Next**. This application can be used to integrate with Tencent Cloud to implement Okta SSO to the Tencent Cloud console for resource management.

Configuring SAML for the Okta application

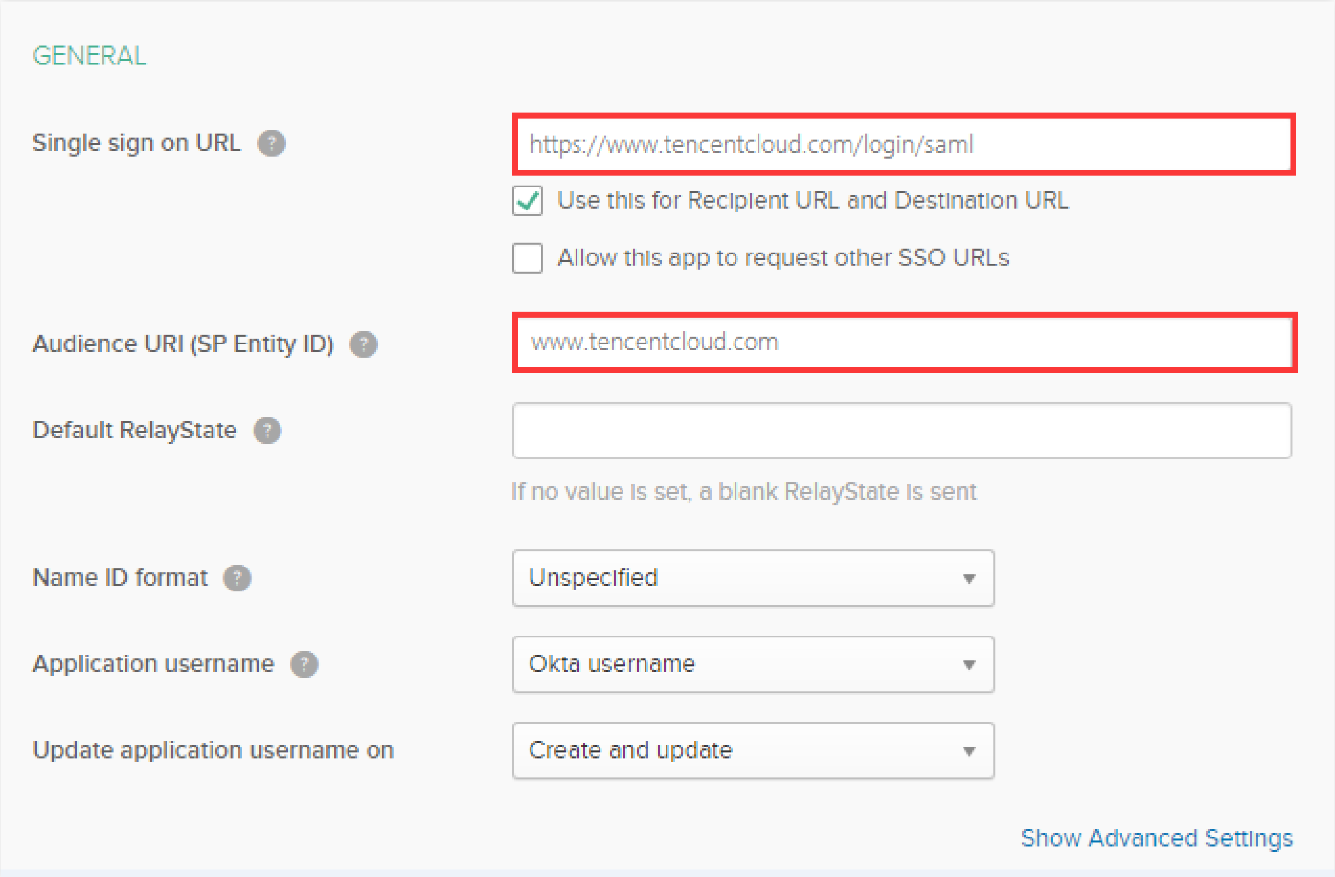
Note:

©2013-2022 Tencent Cloud. All rights reserved.

This step maps Okta application attributes to Tencent Cloud attributes to create trust between Okta and Tencent Cloud.

If you followed the steps in Creating an Okta application to create your application, you can go straight to step 3.

1. Go to the application management page, and click the name of the application you created.
2. On the **General** page, click **Edit** in the **SAML Settings** section, confirm the current **App name**, **App logo** (optional), and **App visibility** (optional), and click **Next** to enter the **Configure SAML** page.
3. In the **Co**
nfig
ure SAML page, add the following information to **Single sign on URL** and **Audience URL(SP Entity ID)** under **GENERAL** as shown below:



GENERAL

Single sign on URL: https://www.tencentcloud.com/login/saml

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): www.tencentcloud.com

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

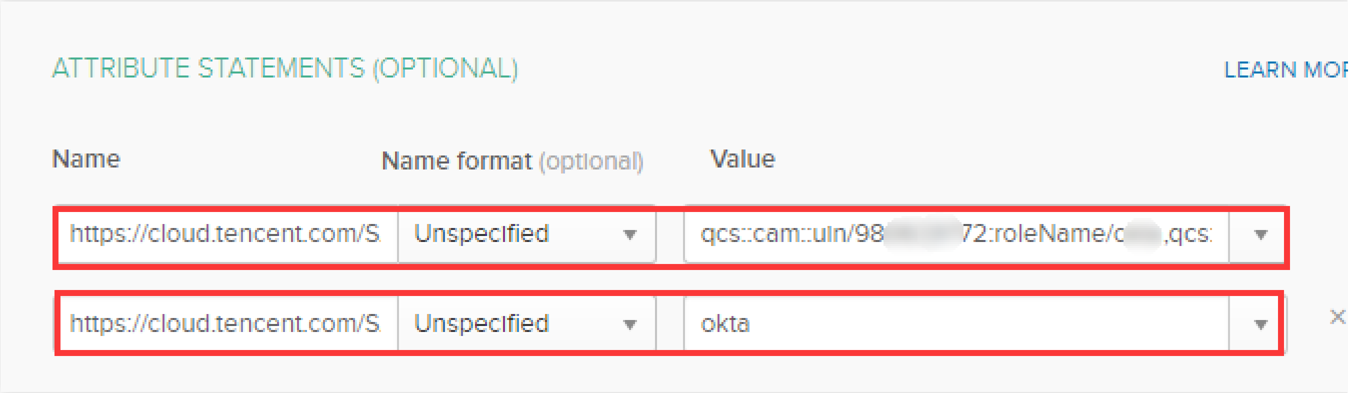
Update application username on: Create and update

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

Site	Single sign on URL	Audience URL(SP Entity ID)
Tencent Cloud International	https://www.tencentcloud.com/login/saml	www.tencentcloud.com

4. In the **Configure SAML** page, add the following information to **ATTRIBUTE STATEMENTS** under **GENERAL** as shown below:

©2013-2022 Tencent Cloud. All rights reserved.



ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Value
https://cloud.tencent.com/S	Unspecified	qcs::cam::uin/98[redacted]72:roleName/c[redacted],qcs:
https://cloud.tencent.com/S	Unspecified	okta

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

Note:

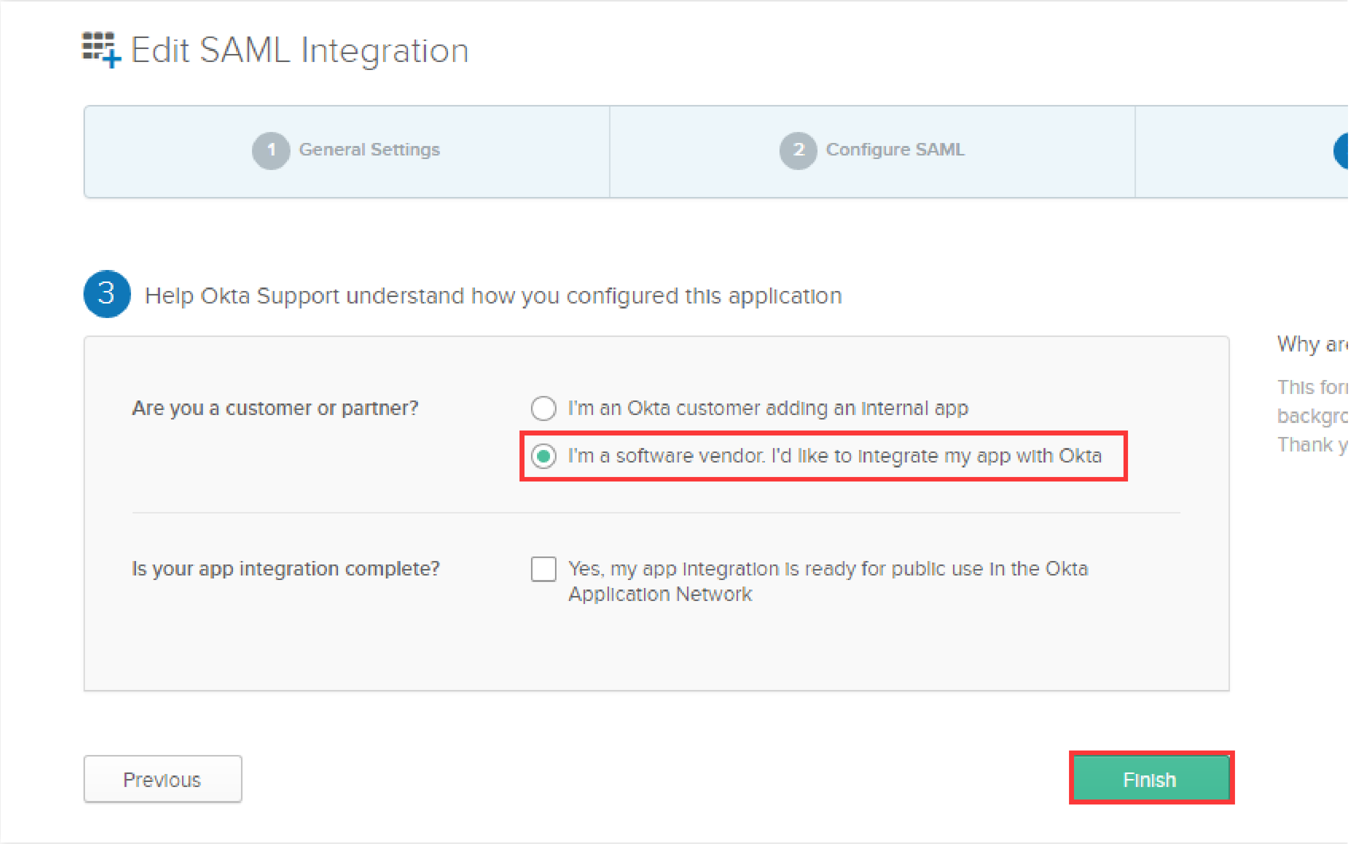
Replace {AccountID}, {RoleName}, and {ProviderName} under **Value** with the following content:

{AccountID}: Replace this with your Tencent Cloud account ID. You can view this in Account Information in the console.

{RoleName}: Replace this with the role name you have created in Tencent Cloud for the IdP. For more information, see Creating Role. Role names can be viewed in Role in the console. If you need to add more, you can add them in this format: qcs::cam::uin/{AccountID}:roleName/{RoleName}. Separate them by semicolons.

{ProviderName}: Replace this with the SAML IdP name that you created on Tencent Cloud. You can view this in IdPs in the console.

5. Click **Next** to enter the **Feedback** page. Select the following information and click **Finish** to complete the CAM configuration as shown below:



Edit 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

Is your app integration complete?

□ Yes, my app integration is ready for public use in the Okta Application Network

Why ar

This for
backgro
Thank y

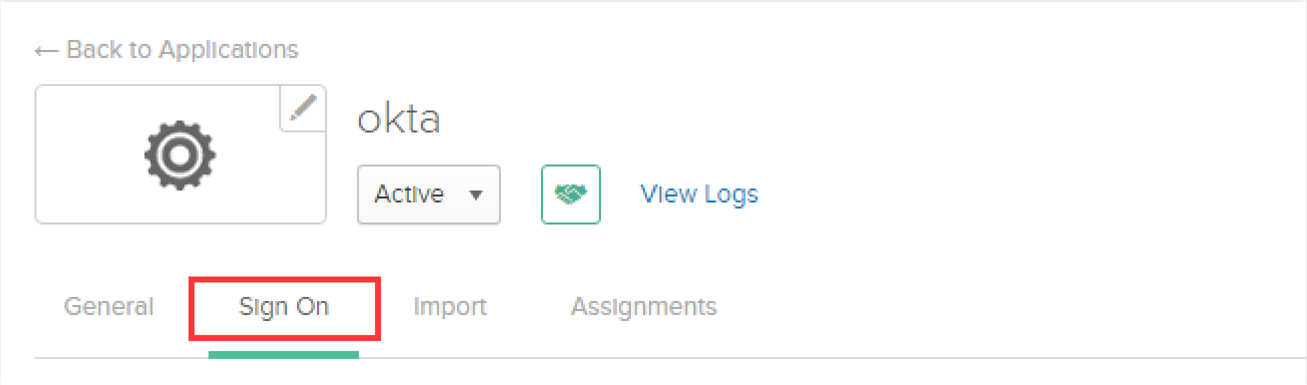
Configuring SAML integration for the Okta application

Note:

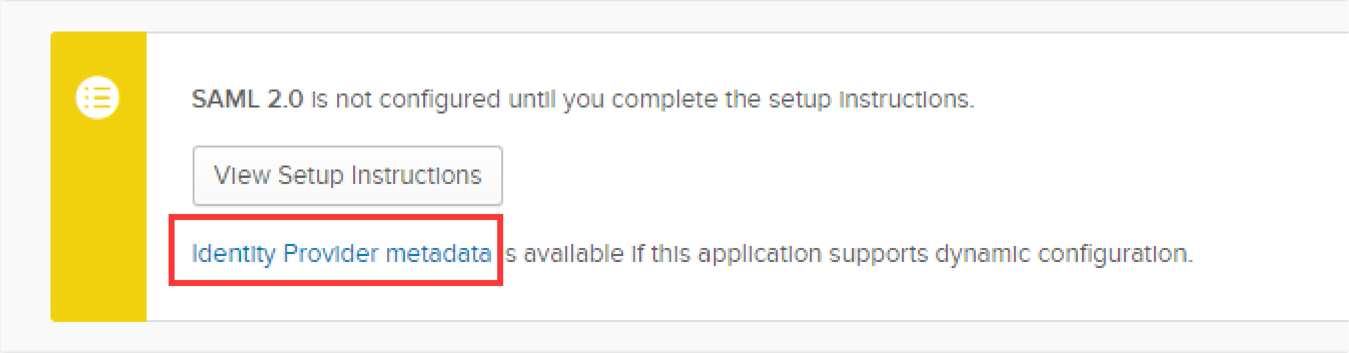
This step configures the trust relationship between Okta and Tencent Cloud.

1. Log in to Admin page, and select **Applications** to go 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. Click **Sign On** as shown below:



3. On the **Sign On** page, click **Identity Provider metadata** to view the metadata of the IdP as shown below:



SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

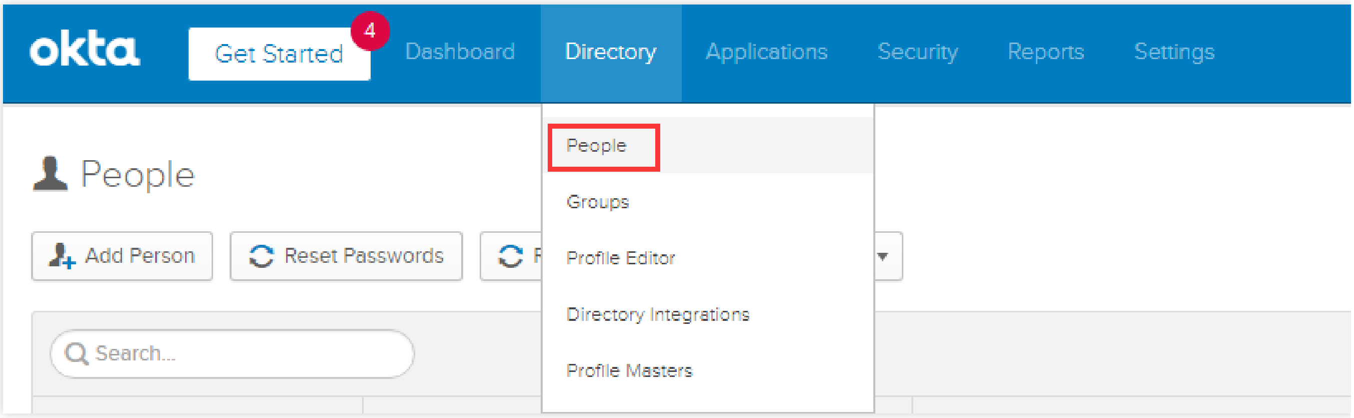
4. After obtaining the identity provider metadata, you can right click on the viewing page to save it locally.
5. Create the SAML identity provider and roles in Tencent Cloud. For more information, see Creating IdP.

Configuring an Okta user

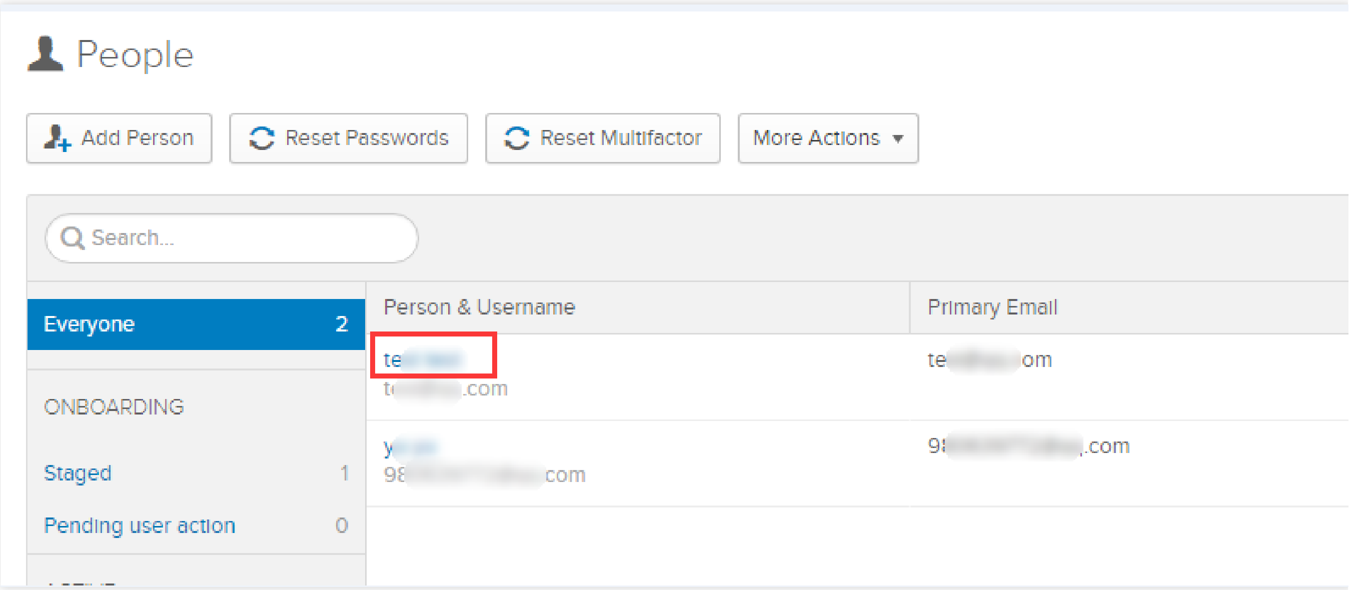
Note:

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

1. Log in to the Admin page and click **Directory** > **People** to enter the user management page as shown below:

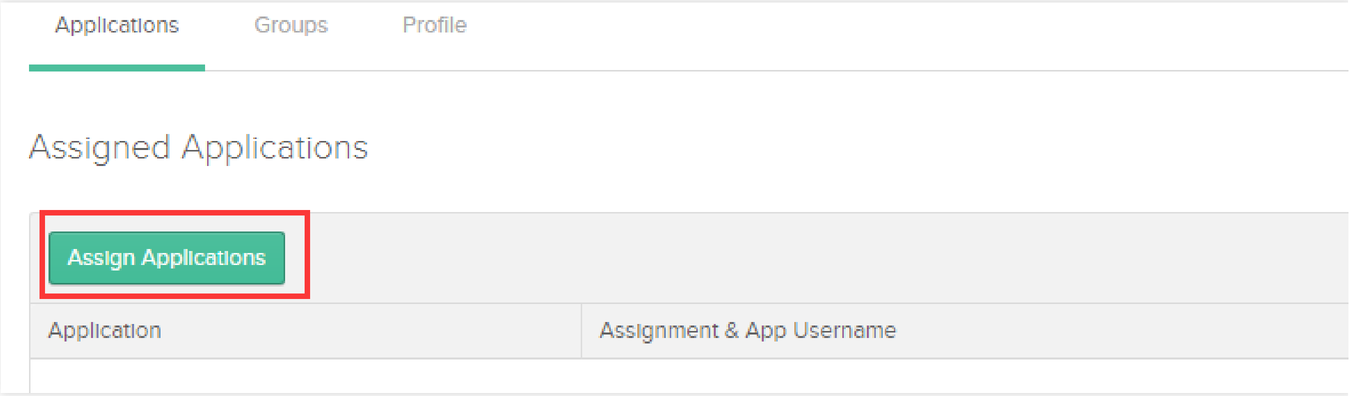


2. On the user management page, click **Everyone** in the top-left corner. Locate the target user as shown below:

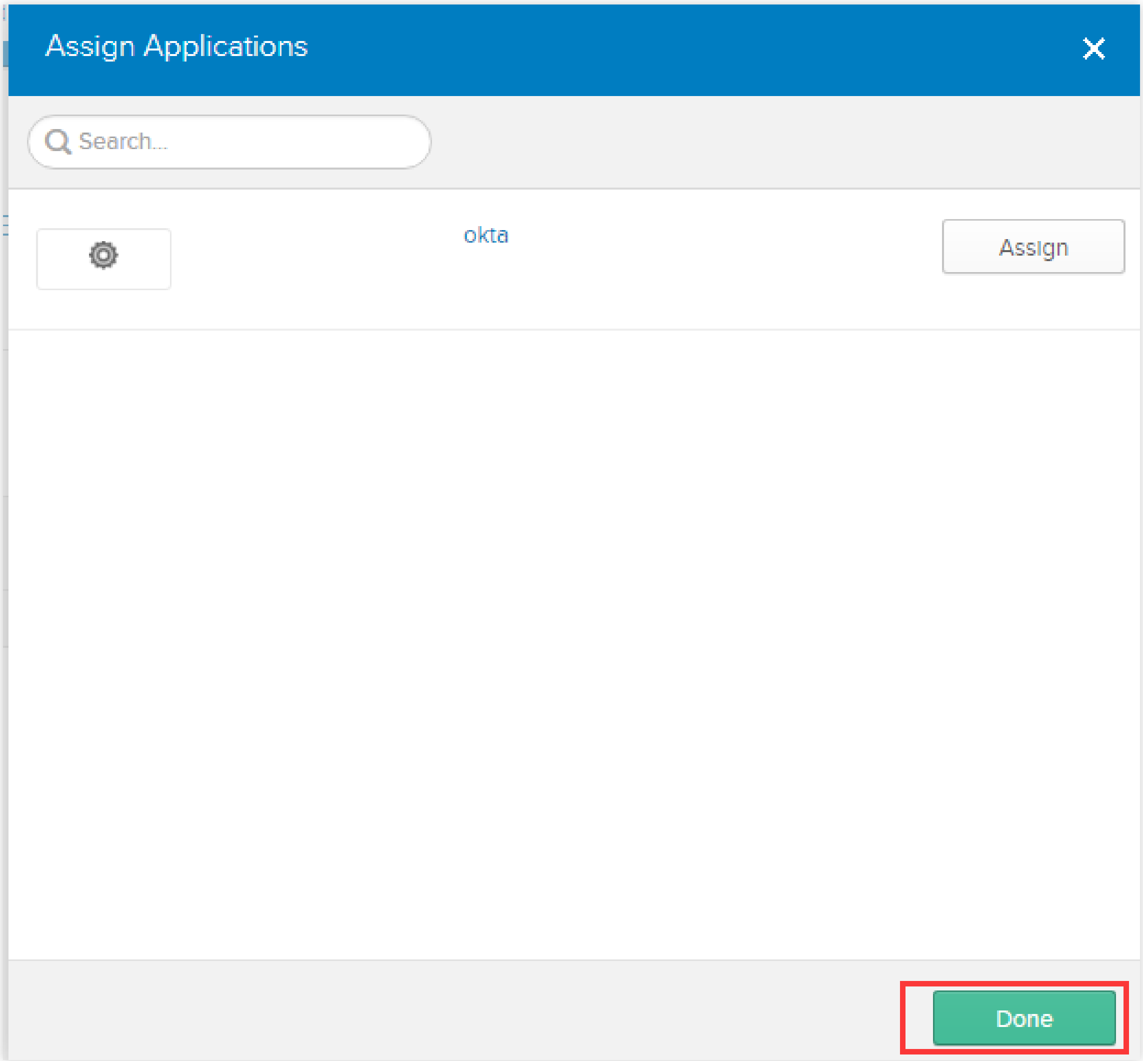


Person & Username	Primary Email
te[redacted] t[redacted].com	te[redacted]om
y[redacted] 98[redacted]com	9[redacted].com

3. Click the username to enter the user details page. Click **Assign Applications** in the top-left corner as shown below:



4. In the **Assign Applications** pop-up window, click **Done** to complete the configuration of the Okta user as shown below:



5. Go to the application management page , and click the name of the application you created to enter 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.

ADFS SSO to Tencent Cloud

Last updated：2024-01-23 17:46:25

Overview

Microsoft Windows Server's Active Directory Federation Services (ADFS) is a new technology for authenticating users of multiple web applications during one session. Tencent Cloud supports identity federation with Security Assertion Markup Language 2.0 (SAML 2.0). SAML 2.0 is an open standard used by many identity providers (IdPs). SAML 2.0-based federation can be used to integrate ADFS with Tencent Cloud. Then, federated single sign-on (SSO) can be implemented by using an ADFS account, and admins can authorize users that have their federated identity authenticated to log in to the Tencent Cloud console for resource management, eliminating the need to create a CAM sub-user for each employee in the organization.

Prerequisites

You have a Windows Server CVM instance. For more information on how to purchase one, see Billing Overview.
You have entered the **Server Management** > **Dashboard** page and found the **Add Roles and Features Wizard** in your computer (see Install or Uninstall Roles, Role Services, or Features).
You have a verified domain name.

Directions

Installing the AD domain services and DNS services

1. On the dashboard management page, click **Add Roles and Features**, keep the default settings for options on the page, and click **Next** repeatedly to enter the **Add Roles and Features Wizard** page.
2. On the **Add Roles and Features Wizard** page, keep the default settings for options on the page, and click **Next** repeatedly.
Th
en, select **Active Directory Domain Services** and **DNS Server** on the **Server Roles** page.
3. Keep the default settings for options on the page, click **Next** repeatedly, and click **Install**. On the page indicating the successful installation, click

⚠ in the top-right corner.

4. Click **Promote this server to a domain controller** to go to the deployment configuration page.
5. Click **Next**. After the installation is completed, enter the password. Keep the default settings for options on the page and click **Next** repeatedly.
6. Click **Install** and restart the server after the installation is completed.
7. At this point, the AD domain services and DNS service have been installed, and the server has been promoted to a domain controller.

Installing the web server

1. Refer to step 2 in **Installing the AD domain services and DNS services** to enter the **Server Roles** page. Select **Web Server**.
2. Keep the default settings for options on the page and click **Next** > **Install** repeatedly to install the web server.

Applying for a certificate

If you already have an SSL certificate, you can directly install ADFS.

1. Click the **Windows** icon in the bottom-left corner, enter the "mmc" command in the search box, and press **Enter** to run it and access the **Console 1-[Console Root]** page.
2. On the **Console 1-[Console Root]** page, click **File**>**Add**/**Remove Snap-in**, select a certificate in the pop-up window, and click **Add**>* *Finish**.
3. Click **Certificates - Current User**. I

n the e

xpanded directory, right-click **Personal**, click **All Tasks** > **Advanced Operations** > **Create Custom Request**.
4. Keep the default settings for options on the page, click **Next** repeatedly to enter the **Certificate Enrollment** page, and click **Proceed without enrollment policy**.
5. On the **Custom request** page, select the following information:

Template: (No template) Legacy key

Request format: PKCS#10

6. Click **Details** > **Properties**. On the **General** tab, enter a friendly name and description.
7. On the **Subject** tab, enter **Value** (`*.example.com` in this example) and click **Add**.
8. On the **Private Key** tab, select **Microsoft RSA SChanel Cyptograhic Provider (Encryption)** and **Make private key exportable**.
9. Click **OK** > **Next**, select the directory for saving the certificate, and click **Finish**.

Installing an ADC (AD certificate server)

1. Refer to step 2 in **Installing the AD domain services and DNS services** to select **Active Directory Certificate Services**.
2. Keep the default settings and click **Next** repeatedly. On the **Role Services** page, select **Certification Authority** and **Certification Authority Web Enrollment**.
3. Click **Install**. On the page indicating the successful installation, click

⚠ in the top-right corner and click **Configure Active Directory Certificate Services on the destination server**.

4. Keep the default settings for options on the page and click **Next** repeatedly. On the **Role Services** page, select **Certification Authority** and **Certification Authority Web Enrollment**.

5 Keep the default settings for options on the page, click **Next** repeatedly, and click **Configure** to install the ADC.

Generating an SSL certificate

1. Visit http://localhost/certsrv and click **Request a certificate**.
2. On the **Request a Certificate** page, click **advanced certificate request**.
3. On the **Advanced Certificate Request** page, click **Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS#7 file**.
4. Copy and paste the certificate file content saved in **Applying for a certificate** to the input box, select **Web Server** for **Certificate Template**, and click **Submit**.
5. After the application succeeds, click **Download certificate** to download the certificate in both formats.
6. Refer to step 3 in **Applying for a certificate**, right-click **Personal**, and click **All Tasks** > **Import**.
7. Select the certificate file saved in step 5, keep the default settings for options on the page, click **Next** repeatedly, and click **Finish**.
8. Refer to step 3 in **Applying for a certificate**, right-click **Personal**, and click **All Tasks** > **Export**.
9. On the **Certificate Export Wizard** page, select **Yes, export the private key** and **Group or user names (recommended)**, and click **Next** to export the saved file.

Installing the ADFS

1. Refer to step 2 in **Installing the AD domain services and DNS services** to enter the **Server Roles** page. Select **Active Directory Federation Services**.
2. Keep the default settings for options on the page, click **Next** repeatedly, and click **Finish**. On the result page, click **Configure the federation service on this server.**

![](https://main.qcloudimg.com/raw/a68753820c34fef24ab06c1ced2ac729.png

3. Keep the default settings for options on the page, click **Next** repeatedly to enter the **Specify Service Properties** page, and enter and import the following information:

SSL Certificate: Import the certificate file saved in step 9 in **Generating an SSL certificate**.

Federation Service Name: Enter the name of the destination server (same as the name in the top-right corner) or an sts. or .adfs domain name.

Federation Service Display Name: Enter the name displayed during login.

4. On the **Specify Service Account** page, enter an account

name an

d password, keep the default settings for other options, and click **Next** repeatedly until the ADFS is installed successfully.

5. Visit the following link to download the XML file.

```
https://federation service name/federationmetadata/2007-06/federationmetadata.xml
```

6. Run `Set-AdfsProperties -EnableIdpInitiatedSignonPage $True` in PowerShell:

Access the following entry for login:

```
https://federation service name/adfs/ls/idpinitiatedSignOn.htm
```

7. Enter the account name and password configured in step 4 to log in.

Note:

If `400 Bad Request` is returned in the browser, perform the following operations in PowerShell:

Get the user starting the ADFS service, open PowerShell, and run the script `setspn -s http/URL of ADFS server domain controller\\user` . For example, if the full name of the ADFS server is

`172_21_0_13.weezer.club` , the domain controller is `WEEZER` , and the user is `Administrator` , you need to run the script `setspn -s http/172_21_0_13.weezer.club WEEZER\\Administrator` .

Creating an IdP in Tencent Cloud

Note:

You can perform this step to configure the trust between ADFS and Tencent Cloud.

Create a SAML IdP in Tencent Cloud and save the IdP name, which can contain only letters.For
more in
formation, see Creating IdP.

Creating a role for an IdP

Note:

You can perform this step to grant the ADFS user the Tencent Cloud SSO access permission.

Create a role for your IdP and save the role name, which can contain only letters.Fo
r more infor
mation, see Creating Role.

Here, select the IdP created in Creating an IdP in Tencent Cloud.

Configuring a user and user group

1. On the **Dashboard** page in the Server Manager, click **Tools** in the top-right corner and select **Active Directory Users and Computers**.
2. On the **Active Directory Users and Computers** page, click **Action** > **New** > **Group**.
3. On the **New Object - Group** page, enter the group name.

Note:

Replace **your root account ID** with your Tencent Cloud account ID, which can be viewed in **Account Center** in the console.

Replace **Tencent Cloud role name** with the role name created for the IdP in Tencent Cloud.

4. On the **Active Directory Users and Computers** page, click **Action** > **New** > **User**.
5. Create an employee, enter the basic employee information, set a username that can contain only letters, and save the username.
6. On the **Active Directory Users and Computers** page, find the new user in the **Users** directory and add the user to the user group.

Configuring a mapping rule

1. On the **AD FS** page in the Server Manager, click **Tools** in the top-right corner.
2. Select **AD FS Management** and click **Add Relying Party Trust**.
3. On the **Add Relying Party Trust Wizard** page, select **Claims aware** and click **Start**.
4. Visit the following link to download the XML file provided by Tencent Cloud IdP.

```
https://cloud.tencent.com/saml.xml
```

5. Import the file of the Tencent Cloud IdP.

6. Keep the default settings for options on the page, click **Next** repeatedly, and click **Finish**.

7. Click **Relying Party Trusts** > **Edit Claim Issuance Policy** > **Add Rule**.

8. On the **Add Transform Claim Rule Wizard** page, click **Choose Rule Type** > **Transform an Incoming Claim** > **Next**.

9. On the **Configure Rule** page, enter the rule information and click **OK**.

Note:

Claim rule name: Enter `NameID` .

Incoming claim type: Select **Windows account name**.

Outgoing claim type: Select **Name ID**.

Outgoing name ID format: Select **Persistent Identifier**.

Select **Pass through all claim values**.

10. On the **Add Transform Claim Rule Wizard** page, click **Choose Rule Type** > **Send Claims Using a Custom Rule** > **Next**.

11. On the **Configure Rule** page, enter the rule information and click **OK**.

Note:

Claim rule name: Enter `Get AD Groups` .

Custom rule: Add the following information:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountn
=> add(store = "Active Directory", types = ("http://temp/variable"), query = ";toke
```

12. On the **Add Transform Claim Rule Wizard** page, click **Choose Rule Type** > **Send Claims Using a Custom Rule** > **Next**.

13. On the **Configure Rule** page, enter the rule information and click **OK**.

Note:

Claim rule name: Enter `Role` .

Custom rule: Add the following information:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountn
=> add(store = "Active Directory", types = ("http://temp/variable"), query = ";toke
```

Here, replace IdP name with the name of the IdP created in Creating an IdP in Tencent Cloud.

14. On the **Add Transform Claim Rule Wizard** page, click **Choose Rule Type** > **Send Claims Using a Custom Rule** > **Next**.

15. On the **Configure Rule** page, enter the rule information and click **OK** as shown below:

Note:

Claim rule name: Enter `RoleSessionName` .

Custom rule: Add the following information:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^Tencent-([\\d]+)"]
 => issue(Type = "https://cloud.tencent.com/SAML/Attributes/RoleSessionName", Value
```

Note:

To enable SSO to Tencent Cloud in another browser other than the ADFS server, you can configure a subdomain (your federation service name) at your IdP for access and login.

©2013-2022 Tencent Cloud. All rights reserved.

Implementing OIDC-Based Role-Based SSO

Last updated：2024-01-23 17:46:25

Before implementing the OpenID Connect (OIDC)-based role-based single sign-on (SSO), you need to create an identity provider (IdP) and create a role for it in the Tencent Cloud console, and then use the OIDC token issued by the IdP to obtain the Tencent Cloud STS token (the role’s temporary key).

Creating an OIDC IdP

1. On the left sidebar in the CAM console, select **Identity Providers** > **Role-Based SSO**.
2. On the **Role-Based SSO** page, click **Create IdP**.
3. On the page you enter, select “OIDC” as the IdP type and enter the following IdP information:

IdP Name: The custom IdP name that is unique under a Tencent Cloud account.

IdP URL: The OIDC IdP identifier provided by an external IdP. It must be a standard URL that starts with “http”.

Client ID: The client ID registered in the OIDC IdP. You can configure multiple client IDs if multiple applications need to access Tencent Cloud.

Public Key for Signature: The public key used to verify the signature of the OIDC IdP ID token. It corresponds to the value of the `jwks_uri` field in the OIDC metadata document. Please open the URL in your browser to obtain the public key. We suggest you rotate it timely.

Remarks: Remarks for the IdP.

4. Click **Next** to enter the information review page.
5. Confirm the information you entered and click **Complete** to save it.

Creating a role for the IdP

1. On the left sidebar in the CAM console, click **Roles**.
2. On the role management page, click **Create Role**.
3. Select **IdPs** as the role entity.
4. On the page you enter, select “OIDC” as the IdP type.
5. Select an IdP you created.
6. Set conditions for the role:

oidc:iss: The OIDC issuer, which is required. The conditional operator must be `string_equal` , and the value must be the IdP URL you entered for the selected OIDC IdP. The role can be assumed only if the value of the `iss` field in the OIDC token meets this condition.

©2013-2022 Tencent Cloud. All rights reserved.

oidc:aud： The OIDC audience, which is required. The conditional operator must be `string_equal` , and the value(s) must be the client ID(s) you configured for the selected IdP. The role can be assumed only if the value of the `aud` field in the OIDC token meets this condition.
oidc:sub: The OIDC subject, which is optional. The conditional operator can be a string of all types, and you can specify up to 10 values for this condition. The role can be assumed only if the value of the `sub` field in the OIDC token meets this condition.

7. Click **Next**.
8. On the page you enter, associate permissions policies with the role and click **Next**.
9. On the review page, enter the role name and role description (optional) and click **Complete** to save the above configurations.

Obtaining the OIDC token issued by the IdP

You cannot log in to the Tencent Cloud console using OIDC. Instead, you must implement OIDC-based SSO through programmatic access, that is, you need to call an API to obtain the temporary key and use the temporary key to access Tencent Cloud. As the OIDC token generation process is essentially based on OAuth, you need to use OAuth 2.0 to obtain the OIDC token from an OIDC IdP such as Okta. For more information, see the IdP-related documentation.

Using the OIDC token to obtain the STS token

After you get the OIDC token from the IdP, you can directly call the AssumeRoleWithWebIdentity API to obtain the STS token to access Tencent Cloud.
Sample request:

©2013-2022 Tencent Cloud. All rights reserved.

```
POST / HTTP/1.1
Host: sts.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: AssumeRoleWithWebIdentity
<Common request parameters>

{
    "DurationSeconds": "5000",
    "RoleSessionName": "test_OIDC",
    "WebIdentityToken": "eyJraWQiOiJkT*********CNOQ",
    "RoleArn": "qcs::cam::uin/798950673:roleName/OneLogin-Role",
    "ProviderId": "OIDC"
}
```

Sample response:

```
{
  "Response": {
    "ExpiredTime": 1543914376,
    "Expiration": "2018-12-04T09:06:16Z",
    "Credentials": {
      "Token": "1siMD5r0tPAq9xpR******6a1ad76f09a0069002923def8aFw7tUMd2nH",
      "TmpSecretId": "AKID65zyIP0mp****qt2SlWIQVMn1umNH58",
      "TmpSecretKey": "q95K84wrzuE****y39zg52boxvp71yoh"
    },
    "RequestId": "f6e7cbcb-add1-47bd-9097-d08cf8f3a919"
  }
}
```

Using the STS token to access Tencent Cloud resources

You can now use the STS token you obtained in the above steps to access Tencent Cloud resources for which you have permissions.

Access Key

Root Account Access Key Management

Last updated：2023-12-19 14:21:50

Note:

To reduce the risk of key exposure, as of November 30, 2023, the function to query SecretKey for all root accounts and sub-accounts will be closed, which can only be kept at the time of creation. Please keep your SecretKey in time.

Overview

Access keys, also known as API keys, are the security certificates required for user identity verification when accessing Tencent Cloud APIs. They are composed of both a SecretId and a SecretKey. If a user does not possess an API key, it is necessary to create one within the API key management system, otherwise, they will be unable to invoke the cloud API interface.

This document describes how to create, enable/disable and delete API keys for the root account as wel as view API key information of the root account.

Note:

Access keys are utilized for API call access. Given that the root account possesses full control over its resources, you'd better not create access keys for root accounts and use them for routine tasks in order to reduce the security risks associated with access key leakage.

Prerequisites

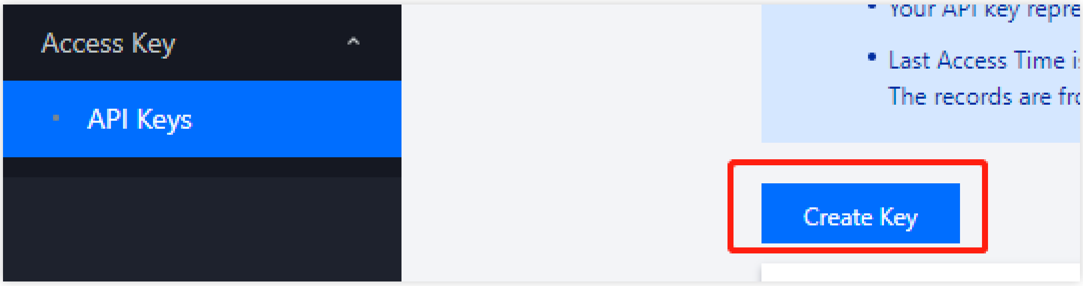
Log in to the CAM console by using a root account. Choose **Cloud Access Management > Access Key > API Keys.**

Directions

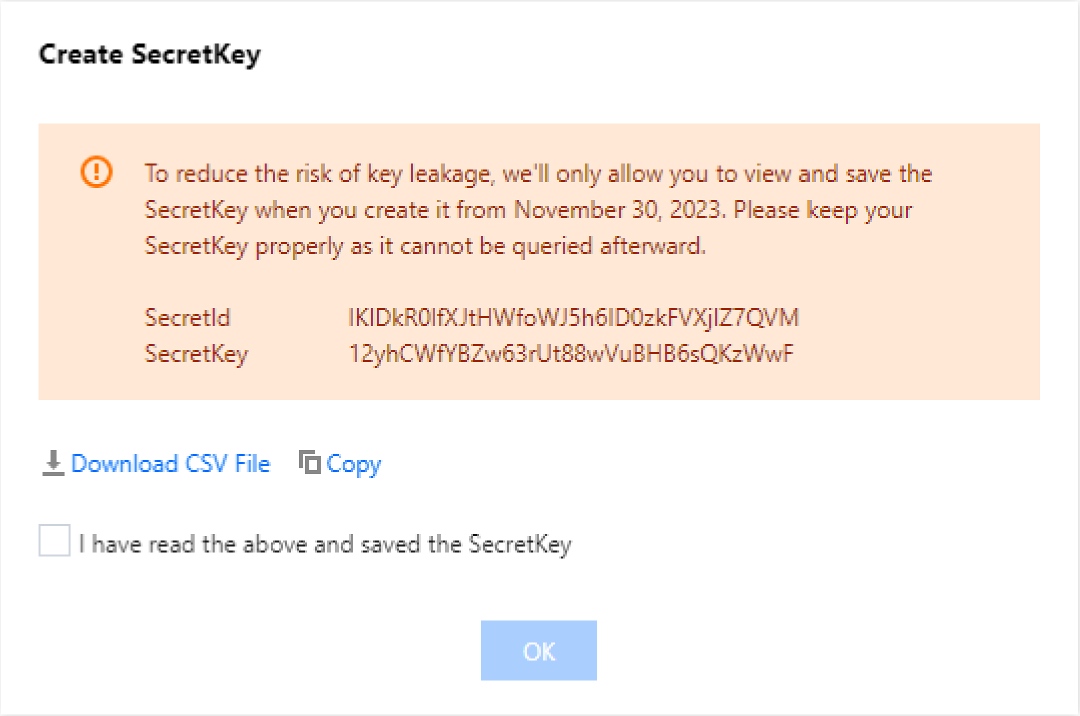
Creating an API key for a root account

You can create an API key for a root account. After the API key is created, the root account can use APIs, SDKs, or other development tools to manage the resources under the account.

1. Click **Create Key** in the upper left corner of the API Keys Management page, as shown below:



2. In the pop-up window of **Create SecretKey**, the key you've created will be displayed. Please keep your SecretId and SecretKey well. As of November 30, 2023, the created keys will only provide the SecretKey when created, and can not be queried afterward.



Create SecretKey

To reduce the risk of key leakage, we'll only allow you to view and save the SecretKey when you create it from November 30, 2023. Please keep your SecretKey properly as it cannot be queried afterward.

SecretId	IKIDkR0lfXJtHWfoWJ5h6ID0zkFVXjIZ7QVM
SecretKey	12yhCWfYBZw63rUt88wVuBHB6sQKzWwF

Download CSV File Copy

□ I have read the above and saved the SecretKey

OK

Note：

One root account can create up to 2 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.

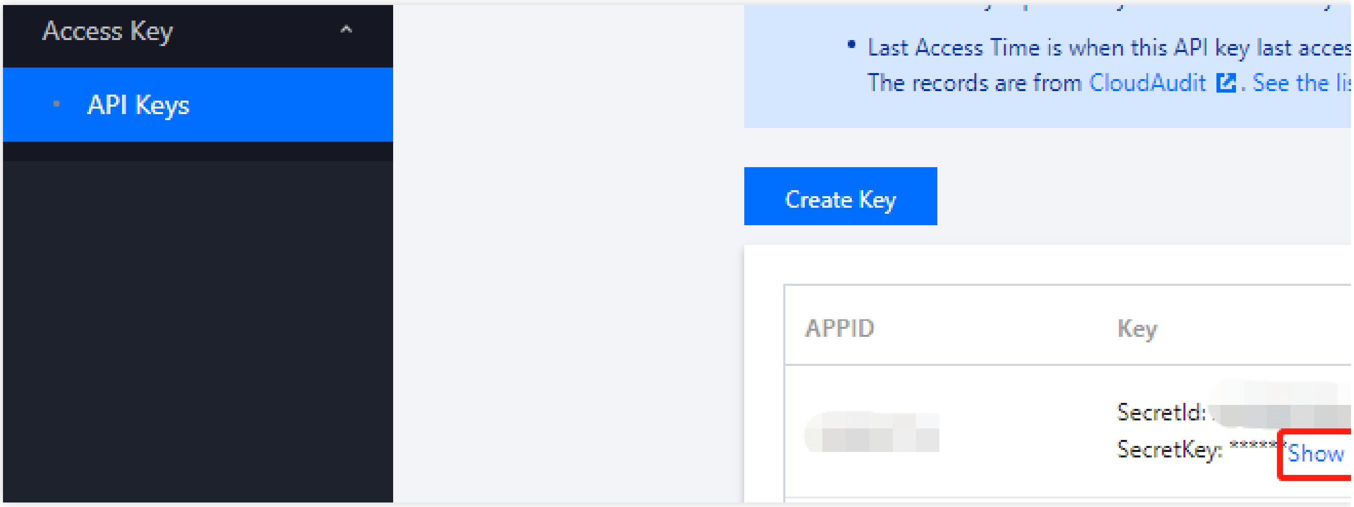
API keys are important credentials for creating Tencent Cloud API requests. To keep your assets and services secure, keep your keys appropriately, and change them regularly. Please remember to delete the old keys after creating new ones.

Viewing an API key of a root account

©2013-2022 Tencent Cloud. All rights reserved.

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

1. On the API Keys Management page, you can directly get and copy `SecretId` under the **Key** column.
2. Click **Show** in the **Key** column. You can get and copy `SecretKey` after completing identity verification. (To reduce the risk of key exposure, as of November 30, 2023, the function to query SecretKey for all root accounts and sub-accounts will be closed, which can only be kept at the time of creation. Please keep your SecretKey in time.)



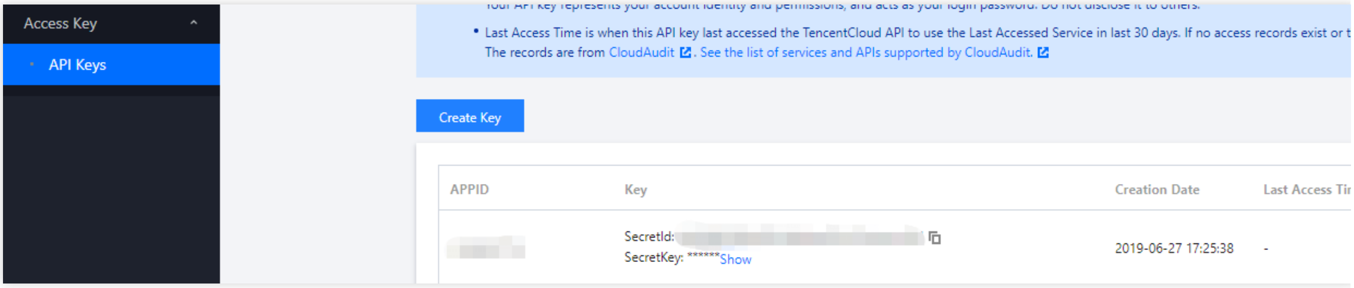
- Last Access Time is when this API key last acces
The records are from CloudAudit . See the lis

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

Disabling/enabling an API key of a root account

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. Click **Disable** on the API Keys Management page.



Your API key represents your account identity and permissions, and acts as your login password. Do not disclose it to others.

- 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 t
The records are from CloudAudit . See the list of services and APIs supported by CloudAudit.

APPID	Key	Creation Date	Last Access Ti
[redacted]	SecretId: [redacted] SecretKey: ******Show	2019-06-27 17:25:38	-

2. In the pop-up window, click **Confirm** to disable the access key.

Note：

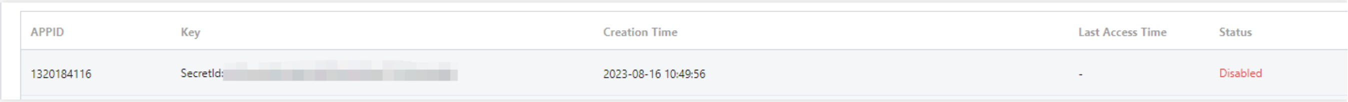
You can click **Enable** in the **Operation** column to enable the key. After the key is enabled, you can use APIs, SDKs, or other development tools to manage the resources under the account.

Deleting an API key of a root account

1. Click **Disable** on the API Keys Management page. If the target API key was disabled, you can go to Step 3.

2. In the pop-up window, click **Disable**.

3. On the API Key Management page, click **Delete** in the **Operation** column.



APPID	Key	Creation Time	Last Access Time	Status
1320184116	SecretId:[redacted]	2023-08-16 10:49:56	-	Disabled

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

Note：

Please note that a deleted API key cannot be restored.

Access Key

Last updated：2023-12-19 14:21:43

Note：

To reduce the risk of key exposure, as of November 30, 2023, the function to query SecretKey for all root accounts and sub-accounts will be closed, which can only be kept at the time of creation. Please keep your SecretKey in time.

Operation Scenarios

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

Prerequisites

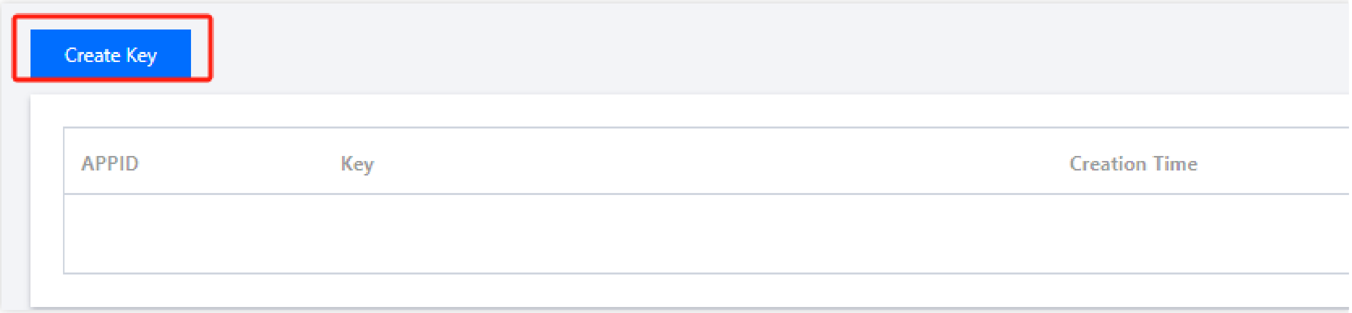
Log in to the CAM Console and go to User List. Find the sub-user or collaborator that needs to be configured and click **Username** to enter the user details page.

Directions

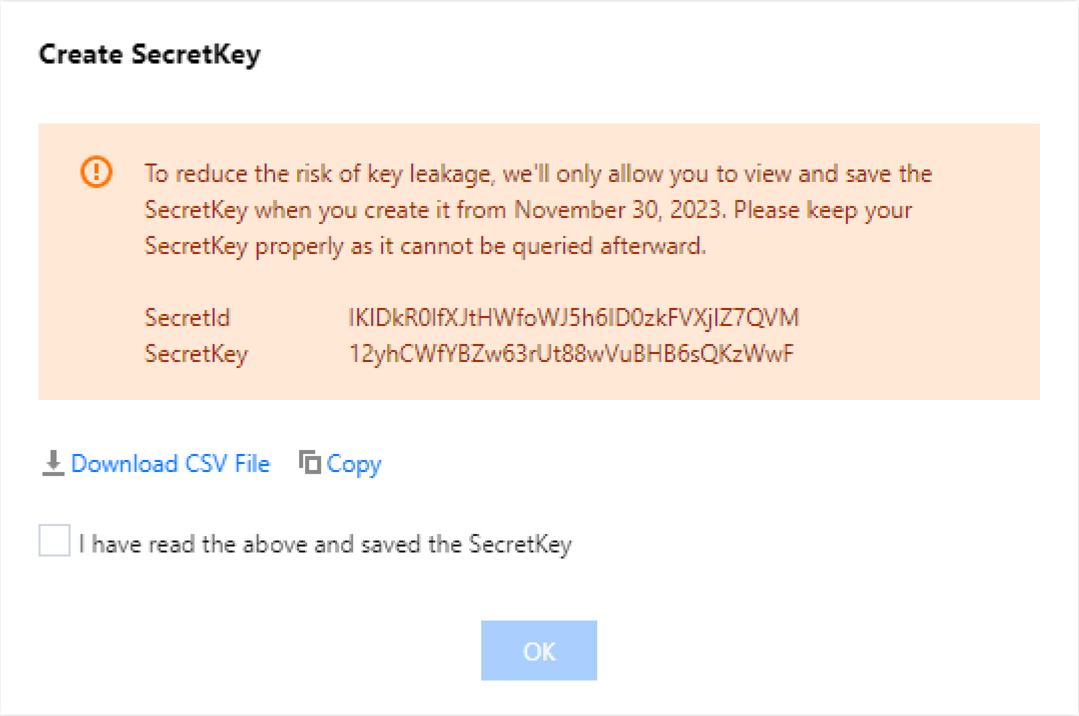
Creating an API key for a sub-account

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 development 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 enter the **API key management** page.
2. On the **API key management** page, click **Create Key**.



3. In the pop-up window of **Create SecretKey**, the key you've created will be displayed. Please keep your SecretId and SecretKey well. As of November 30, 2023, the created keys will only provide the SecretKey when created, and can not be queried afterward.



Create SecretKey

To reduce the risk of key leakage, we'll only allow you to view and save the SecretKey when you create it from November 30, 2023. Please keep your SecretKey properly as it cannot be queried afterward.

SecretId IKIDkR0IfXJtHWfoWJ5h6ID0zkFVXjIZ7QVM
SecretKey 12yhCWfYBZw63rUt88wVuBHB6sQKzWwF

Note:

Each sub-user/collaborator can have at most two API keys.

An API key is an important credential for creating TencentCloud API requests. For the security of your assets and services, please keep the keys private, change them regularly, and delete old keys promptly after creating new ones.

Viewing a sub-account API key

You can view and copy the `SecretId` and `SecretKey` information of a sub-user/collaborator API key. The sub-user/collaborator can use the `SecretId` and `SecretKey` to use APIs, SDKs, or other development tools to manage resources under the root account within the scope of the configured permissions.

1. On the user details page, click **API Keys** to enter the API key management page.

2. On the API key management page, perform the following operations to view and copy the `SecretId` and `SecretKey` information of the API key. An API key is an important credential for creating TencentCloud API requests. For the security of your assets and services, please keep the keys private, change them regularly, and delete old keys promptly after creating new ones.

SecretId: this can be directly viewed in the **Key** column. Click

⧉ to copy and save it.

SecretKey: click **Show** in the **Key** column. You will be able to view it after being authenticated. Click

⧉ to copy and save it. (To reduce the risk of key exposure, as of November 30, 2023, the function to query SecretKey for all root accounts and sub-accounts will be closed, which can only be kept at the time of creation. Please keep your SecretKey in time.)

Disabling/Enabling a sub-account API key

You can disable an API key of a sub-user/collaborator. Please do so with caution as Tencent Cloud will block all requests that use the API key after it is disabled.

1. On the user details page, click **API Key** to enter the API key management page.
2. On the API key management page, click **Disable** in the **Operation** column.
3. In the confirmation window that pops up, click Confirm to disable the access key.

Note:

You can click **Enable** in the **Operation** column to enable the key. After the key is enabled, the sub-account/collaborator can use APIs, SDKs, or other development tools to manage the resources under the root account within the scope of the configured permissions.

Deleting a sub-account API key

1. On the user details page, click **API Key** to enter the API key management page.
2. On the API key management page, click **Disable** in the "Operation" column. If the API key that you want to delete has already been disabled, proceed to step 4.
3. In the confirmation window that pops up, click **Confirm**.
4. On the API key management page, click **Delete** in the "Operation" column to delete the API key.

Note:

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

Related Documents

For more information on how to query sub-account information through the `SecretId` of an access key, please see Searching for Sub-users with Search Box and Searching for Collaborators with Search Box.

User Groups

Creating User Group

Last updated：2024-01-23 17:49:51

Overview

A user group is a set of multiple users (sub-accounts) with the same function. The root account and sub-accounts with admin permissions can create different user groups based on business needs to batch authorize users and set message subscriptions for better management of users and their permissions.

This document describes how to create a user group and associate a policy with it. You can assign your users into different groups for easier management. Users in a user group can manage the resources of the root account within the scope of the group's permissions.

Directions

1. Log in to the CAM console and enter the **User Group** page.
2. Click **Create User Group** to enter the user group information page.
3. On the user group information page, enter the user group name (required) and remarks (optional).

Note:

You can search for user groups in the user group list by name or remarks.

4. Click **Next** to enter the user group permission settings page.
5. On the user group permission settings page, select one or more policies that you want to associate.
6. Click **Next** to enter the review page.
7. On the review page, review the settings for the user group and make changes if needed.
8. After confirming that everything is correct, click **Done**.

Related Documents

For more information on how to manage and authorize sub-users through user group, please see Managing User Group and Setting User Group Permissions.

For more information on how to create a sub-user, please see Creating Custom Sub-user.

Associating/Unassociating Policy with/from User Group

Last updated：2024-01-23 17:49:51

Overview

After creating and authorizing a user group, you can associate/unassociate policies with/from it to quickly change its permissions. Sub-accounts in the user group can manage the resources under the root account within the scope of the granted permissions.

When a policy is associated with a user group, all users in it will have the permissions of the policy.

When a policy is unassociated from a user group, all users in it will no longer have the permissions of the policy.

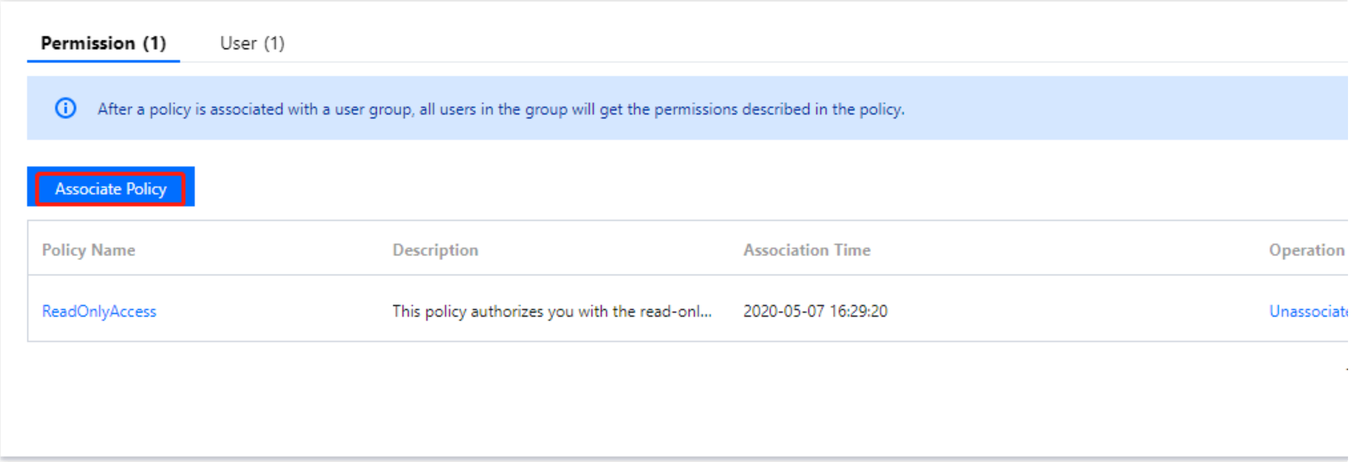
Prerequisites

There is an existing user group (if not, please create one).

Directions

Associating policy with user group

1. Log in to the CAM console and enter 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** module on the user group details page, click **Associate Policy**.



Permission (1) User (1)

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

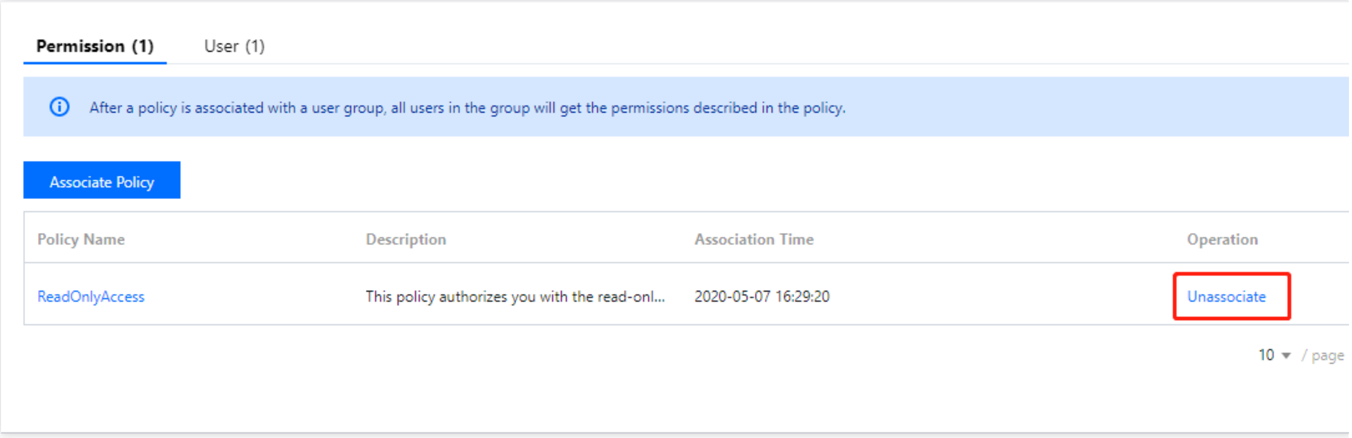
Associate Policy

Policy Name	Description	Association Time	Operation
ReadOnlyAccess	This policy authorizes you with the read-onl...	2020-05-07 16:29:20	Unassociat

4. Select one or more policies to be associated in the pop-up window and click **OK** to associate the policies with the user group.

Unassociating policy from user group

1. Log in to the CAM console and enter 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** module on the user group details page, find the policy to be unassociated and click **Unassociate** on the right.



Permission (1) 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

Policy Name	Description	Association Time	Operation
ReadOnlyAccess	This policy authorizes you with the read-onl...	2020-05-07 16:29:20	Unassociate

10 ▾ / page

4. Click **OK** to unassociate the policy from the user group.

©2013-2022 Tencent Cloud. All rights reserved.

Managing User Groups

Last updated：2024-01-23 17:49:51

Overview

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

When a user is added to a user group, the user will have all the permissions of the user group.

When a user is removed from a user group, the user will no longer have the permissions of the user group.

Prerequisites

There is an existing user group (if not, please create one).

There is an existing sub-account (if not, please create one).

Directions

Adding user to user group

1. Log in to the CAM console and enter the **User Group** page.
2. Find the target user group and click **Add User** in the **Operation** column.
3. In the pop-up window, select the user to be added.
4. Click **OK** to add the user to the user group.

Note:

You can also click the user group name and then add users on the **Users** tab on the details page.

Removing user from user group

1. Log in to the CAM console and enter 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 enter the user list page.
4. Find the user you want to remove, and click **Remove from Group** in the **Operation** column on the right.
5. Click **Remove Users** to remove the user from the user group.

Note:

You can also select users and click **Remove Users** above the user list to remove multiple users at a time.

©2013-2022 Tencent Cloud. All rights reserved.

Deleting User Groups

Last updated：2024-01-23 17:49:51

Overview

This document describes how to delete a user group. After the deletion, sub-accounts in the user group will no longer have the permissions granted to the user group.

Directions

Deleting one single user group

1. Log in to the CAM Console and enter the User Groups management page.
2. On the user group management page, locate the user group to be deleted.
3. Click **Delete** in the "Operation" column on the right to delete the user group.

Role

Role Overview

Last updated：2024-01-23 17:52:00

Role Overview

A role in CAM is a virtual user, which is different from physical users such as sub-accounts, collaborators, or message recipients. Roles can also be granted policies.

A role can be assumed by any Tencent Cloud account and is not exclusively associated with one single account.

Although a root account uses persistent credentials such as a password or access keys when creating a role, the role does not have persistent credentials associated with it. When you assume a role, temporary credentials are created for you to access related resources. Specifically, you can use temporary keys to call open TencentCloud APIs in order to access your Tencent Cloud resources.

Use Cases

Those who can apply for a role are called role entities. Currently, Tencent Cloud role entities are divided into three categories: Tencent Cloud accounts, products and services that support the role feature, and identity providers. The corresponding use cases are as follows:

You want to grant users under your account temporary access to resources or grant users under another Tencent Cloud root account the access to resources under your account.

You may need to allow Tencent Cloud products and services to have access to your resources, but you don't want to embed persistent keys in them, because there may be security issues where it is difficult to rotate keys or keys are leaked after interception.

If you already have an account system for your organization, you can use the Identity Provider (IdP) feature to allow your organization members to access Tencent Cloud resources. This eliminates the need to create a CAM sub-user for each member under your Tencent Cloud account.

©2013-2022 Tencent Cloud. All rights reserved.

Concepts

Last updated：2024-01-23 17:52:00

Before you get started with roles, familiarize yourself with the basic terms, such as role, service role, custom role, role entity, and permission policy. For more terms, please see Glossary.

Role

A role is a virtual identity with a collection of permissions. It is used to grant permissions to role entities for them to access services and resources and perform operations in Tencent Cloud. Those permissions are granted to a role instead of a user or user group.

CAM supports two types of roles:

Service (preset) role: this is a role predefined by a Tencent Cloud service. Once you authorize a service role, the service can assume the role to access and perform operations on your resources.

Custom role: this is a role defined by yourself. You can decide which role entity you want to use and what permissions you want to grant to the role.

Roles can be used by:

Tencent Cloud root accounts that can assume roles.

Tencent Cloud sub-users or collaborators that can assume roles.

Roles can also be used by Tencent Cloud services that support roles. To check whether a Tencent Cloud service supports service roles, please see CAM-Enabled Products.

Service Role

A service role is a special preset CAM role provided directly by a Tencent Cloud service. The permissions associated with a service role are predefined by the corresponding service. Once you grant a service role to a service, it can call other Tencent Cloud services on your behalf within the scope of granted permissions. Service roles make it easier for you to use services, because you do not need to manually add permissions when creating a role. Instead, you only need to decide whether you want to grant a service the permissions associated with a service role.

When you grant a service role to a service, the permissions and role entity corresponding to the service role have already been defined. Unless you redefine the permissions, the service role can only be assumed by its corresponding service. A service role comes with a predefined role name, role entity, and permission policies.

Custom Role

A custom role is a CAM role defined by yourself. You can define the role name, role entity, and permissions, which allows you to manage access to your resources in a more flexible way.

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

Role Entity

A role entity is an object allowed to have the permissions associated with a role. You can edit role entities by adding or deleting objects to allow them to assume roles to access your Tencent Cloud resources or prohibit them from doing so. Tencent Cloud supports two types of role entities: Tencent Cloud accounts and role-enabled Tencent Cloud services. To find out whether a Tencent Cloud service supports service roles, please see CAM-Enabled Products.

Permission Policy

A permission policy is a JSON file on permissions where you can define which operations a role can perform and what resources it can access. This file should conform to the CAM policy syntax rule.

Trust Policy

A trust policy is a JSON file on permissions where you can define which objects can assume a role and what conditions must be met before they can assume a role. This file should conform to the CAM policy syntax rule.

Creating Role

Last updated：2024-01-23 17:52:00

Overview

This document describes how to create a role via the CAM console or APIs. The created role can manage resources under the root account within the scope of permissions.

Prerequisites

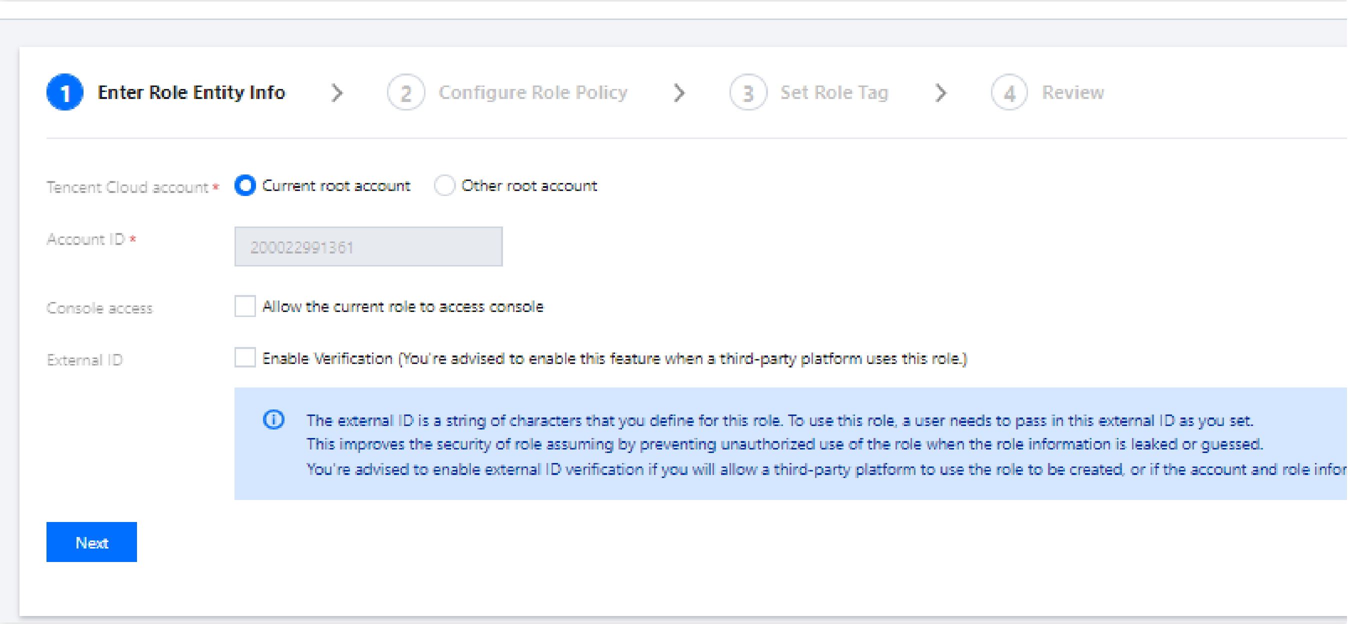
Log in to the CAM console and go to the Roles page.

Directions

Creating in the console

Creating a role for a Tencent Cloud root account

1. On the **Roles** page, click **Create Role**.
2. In the **Select role entity** pop-up window, select **Tencent Cloud Account** as the role entity.



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 infor

3. On the **Enter Role Entity Info** page, enter the following information and click **Next**.

Tencent Cloud account: Select **Current root account** or **Other root account**.

Account ID: Enter the ID of the root account to which you want to grant access to your Tencent Cloud account resources. Your root account ID is entered by default.

Console access: You can select it to allow the current role to access the console.

External ID: We recommend you 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. After it is enabled, you need to enter an external ID.

4. In the policy list, select the policies to be granted to the current role and click **Next**.
5. Set the role tag keys and values and click **Next**.
6. Enter a role name. After confirming that the role entity and policy information are correct, click **Next**.

Note:

If you want to create roles for Tencent Cloud sub-accounts, see Authorizing Sub-account with Role Assuming Policy.

Creating a role for a Tencent Cloud service

1. On the **Roles** page, click **Create Role**.
2. In the **Select role entity** pop-up window, select **Tencent Cloud Product Service** as the role entity.

To check whether a Tencent Cloud service supports using roles, see CAM-Enabled Products.

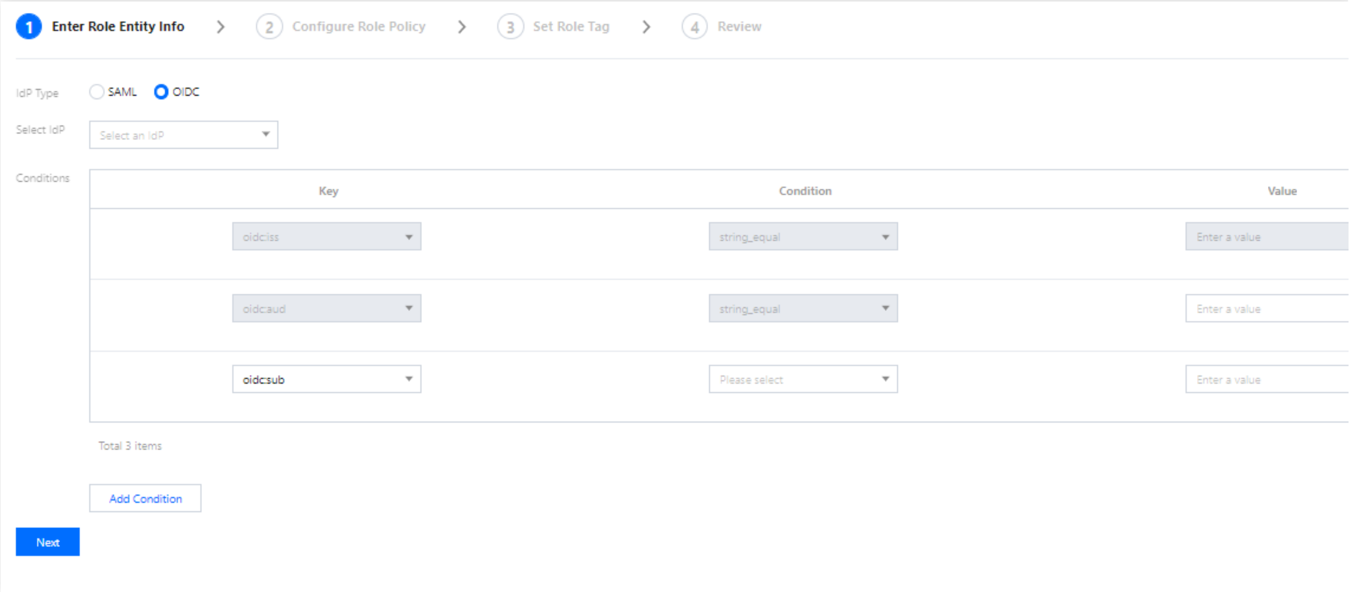
3. Select the service you need as the role entity from the list of services that support roles and click **Next**.
4. In the policy list, select the policies you want to grant the role for permission configuration and click **Next**.
5. Set the role tag keys and values and click **Next**.
6. Enter a role name. After confirming that everything is correct, click **Complete**.

Creating a role for an IdP

1. On the **Roles** page, click **Create Role**.
2. In the **Select role entity** pop-up window, select **IdPs** as the role entity to enter the role information configuration page.

IdPs refer to the identity providers you created. You can select one from them as the role entity.

©2013-2022 Tencent Cloud. All rights reserved.



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
oidc:aud	string_equal	Enter a value
oidc:sub	Please select	Enter a value

Total 3 items

Add Condition

Next

3. Select the IdP type and the specific IdP, configure conditions as needed, and click **Next**.

IdP Type: You can select SAML or OIDC.

Select IdP: You can select an IdP as the role entity.

Console access (optional): You can configure whether to allow the role to log in to the Tencent Cloud console. A role has programming access to Tencent Cloud by default.

Conditions (optional): You can configure conditions for IdPs to use the role. For more information, see Conditions.

4. In the policy list, select the policies you want to grant the role for permission configuration and click **Next**.

5. Set the role tag keys and values and click **Next**.

6. Enter a custom role name. After confirming that everything is correct, click **Complete**.

Creating through APIs

Creating a role for a 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. CompanyExampleA (ownerUin: 12345) calls AttachRolePolicy to associate the new policy with the role `DevOpsRole` . Input parameters: policyName=DevOpsPolicy, roleName=DevOpsRole.

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 IdP

Before creating a role for an IdP, you need to create a SAML IdP in CAM first. For detailed directions, see Creating Role.

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

Note:

The fields in a trust policy are as specified below:

action: Defines the API for which SAML Federation is allowed to use the role. Use `sts:AssumeRoleWithSAML` .

principal: Defines the IdP that is allowed to use the role. Use `{"federated": [ IdPArn ]}` string, such as `"qcs::cam::uin/10001:saml-provider/idp_name"` .

condition: Defines the conditions to be met before an IdP can use the role. `{"StringEquals": {"SAML:aud": "https://cloud.tencent.com/login/saml"}}` is used by default, specifying that only the IdPs with Tencent Cloud as the SAML Federation endpoint are allowed to use this role.

Sample 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 permission policies for the role to be created. For more information on permission policies, see Policy.

3. Call the `cam:CreateRole` API to create a role for the IdP.

Conditions

SAML currently supports the following conditions:

Condition Key	Meaning	Required	Description
saml:aud	Recipient	No	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	No	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	No	This is the statement topic. It contains a value uniquely identifying a user in the organization. The value of this key comes from the `SAML NameID` field in the assertion.
saml:sub_type	External user type	No	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 Key	Meaning	Required	Description
oidc:iss	OIDC issuer	Yes	This condition must use `string_equal`, and the condition value can only be the IdP URL that you entered in the OIDC IdP configuration. The `iss` field of the token of the OIDC IdP account to assume the role must meet this condition.
oidc:aud	OIDC audience	Yes	This condition must use `string_equal`, and the condition value can only be the one or multiple client IDs in the OIDC IdP

			configuration. The `aud` field of the token of the OIDC IdP account to assume the role must meet this condition.
oidc:sub	OIDC subject	No	This condition can be any condition operation in string type, and you can configure up to ten OIDC subjects in the condition value. The `sub` field of the token of the OIDC IdP account to assume the role must meet this condition.

©2013-2022 Tencent Cloud. All rights reserved.

Modifying Role

Last updated：2024-01-23 17:52:00

Introduction

This document describes how to edit and modify role-associated policies and role entities. After the modification, a role can manage the resources under a root account within the scope of updated permissions.

Prerequisites

Log in to the CAM Console and go to the Roles page.

Directions

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. On the role details page, click **Associated Policy** tab to view the policies.
3. Click **Associate Policies**.
4. Select the policies you want to add to the current role from the policy list.
5. Click **OK** to complete editing the policies associated with the role.

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** tab to view the role entity.
3. Click **Manage Entity** to go to Manage Role Entity page. You can make the following modifications according to your needs:

Modifying account: click **Add Account** to add an account (only root account is allowed) as the role entity, or delete an account tag to remove it from the role entities.

Modifying service: select a product service as the role entity, or de-select a product service to remove it from the role entities.

4. Click **OK** to complete editing the role entity.

©2013-2022 Tencent Cloud. All rights reserved.

Using Role

Last updated：2024-01-23 17:52:00

Overview

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

Prerequisites

For example:

Company A wants to outsource its OPS engineer position to company B. The person taking the position needs the access to company A's all CVM resources located in the Guangzhou region.

Company A has an enterprise account `CompanyExampleA` (ownerUin: 12345).

Company B has an enterprise account `CompanyExampleB` (ownerUin: 67890).

Company B has a sub-account `DevB` and wants to use `DevB` to do the work.

Directions

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

Using the role in the console

Using roles through API

1. Company A creates a role for company B (as instructed in Creating a Role).

Select **Tencent Cloud Account** as the role entity and create a role (`DevOpsRole` for example). Then, set company B's enterprise account "67890" as its role entity and add it the permission to manipulate company A's CVM resources in the Guangzhou region.

2. Company B authorizes the sub-account of company B (as instructed in Authorizing a Sub-account with the Policy of Assuming a Role).

Set a policy allowing company B's sub-account `DevB` to use the `DevOpsRole` role of company A (ownerUin: 12345) and grant it the permission of the `sts:AssumeRole` API.

3. Company B's sub-account uses the role to log in to the console.

Log in to the console with company B's sub-account `DevB` and click **Switch Role** in the drop-down list under the profile photo.

Enter company A's root account "12345" and the role name "DevOpsRole". After confirmation, company B can switch to the `DevOpsRole` role of company A (ownerUin: 12345).

©2013-2022 Tencent Cloud. All rights reserved.

You can also switch to other roles by clicking **Switch Role** in the drop-down list.

If you want to return to the original sub-account after switching the role, you can click **Back to Sub-user** in the drop-down list.

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.

Company A takes the following steps as instructed in Creating a Role:

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 permission to manipulate company A's all CVM resources in the Guangzhou region.

Company B takes the following steps as instructed in Authorizing a Sub-account with the Policy of Assuming a Role:

1. Authorize the sub-account `DevB` to assume the `DevOpsRole` role.
2. Call the AssumeRole API to apply for temporary credentials for the role `DevOpsRole` . Input parameters are as follows:

Note:

If company B (`CompanyExampleB`) wants to directly manipulate 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***PCl",
        "tmpSecretKey": "Vpx***MqD"
    },
    "expiredTime": 1506433269,
    "expiration": "2018-09-26T13:41:09Z"
}
```

©2013-2022 Tencent Cloud. All rights reserved.

3. `DevB` can perform operations on company A's resources within the scope of permissions during the validity period of the credentials.
For example, if `DevB` wants to call the DescribeInstances API to view the CVM list, then `DevB` needs to replace the values of `SecretId` and `SecretKey` with the values of `tmpSecretId` and `tmpSecretKey` and set the `Token` in common parameters to the value of `sessionToken` .

Note:

To stop authorizing company B, company A only needs to delete the `DevOpsRole` role.

Deleting a Role

Last updated：2024-01-23 17:52:00

Introduction

This document describes how to delete roles. After being deleted, a role will no longer have the permissions to manage the resources under the root account.

Directions

1. Log in to the CAM Console and go to the Roles page.
2. In the Roles page, select the role you want to delete.
3. Click **Delete** in the operation column and click **OK** to complete the deletion.

Note：

Once a role is deleted, the authorization information associated with the role will also be deleted. Click **OK** to delete the role. The entity of the role, whether it is an account or a service, will no longer be able to use it.

©2013-2022 Tencent Cloud. All rights reserved.

Authorizing Sub-account with Role Assuming Policy

Last updated：2024-01-23 17:52:00

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 enterprise account `CompanyExampleA` (ownerUin: 12345) creates a role with the `CreateRole` API. The entity and name of the role are set to Company B's enterprise account `CompanyExampleB` (ownerUin: 67890) and `DevOpsRole` respectively. CompanyExampleA adds permissions to `DevOpsRole` . For more information, see Creating roles > Creating via APIs.

After being granted the role, Company B's enterprise account (`CompanyExampleB`) wants its sub-account, `DevB` , to perform the job. `CompanyExampleB` needs to authorize `DevB` to assume the `DevOpsRole` role.

1. Create a policy, `AssumeRole` , as follows:

```
}
```

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

2. Associate the policy with the sub-account `DevB` . The sub-account is now granted permissions to assume the `DevOpsRole` role.
3. For more information on how a sub-account can use a role after being granted the permissions, see Using roles.

©2013-2022 Tencent Cloud. All rights reserved.

Resource-based Service Roles

Last updated：2024-01-23 17:52:00

Overview

A role is a virtual identity with an array of permissions. It serves to grant permissions of access to services, operations, and resources within Tencent Cloud to a role carrier. You can associate roles with cloud resources, allowing them to access other cloud product APIs based on Tencent Cloud Security Credential Service STS temporary keys (which can be periodically updated). Compared with direct control via persistent keys, this method further ensures the security of persistent keys under the account and allows more refined control and permission management via role association policies.

Advantages

After a CAM role is bound to cloud resources, the following features and advantages are bestowed:
Access Tencent Cloud's other cloud services through STS temporary keys. For more details, please refer to AssumeRole.
Assign roles with varying access policies to different resources, enabling differentiated access privileges across different cloud services, hence advocating precision granularity in permission control.
Be free from manually saving persistent keys within instances. Access rights can be swiftly altered and maintained by modifying the role's authorization.

Directions

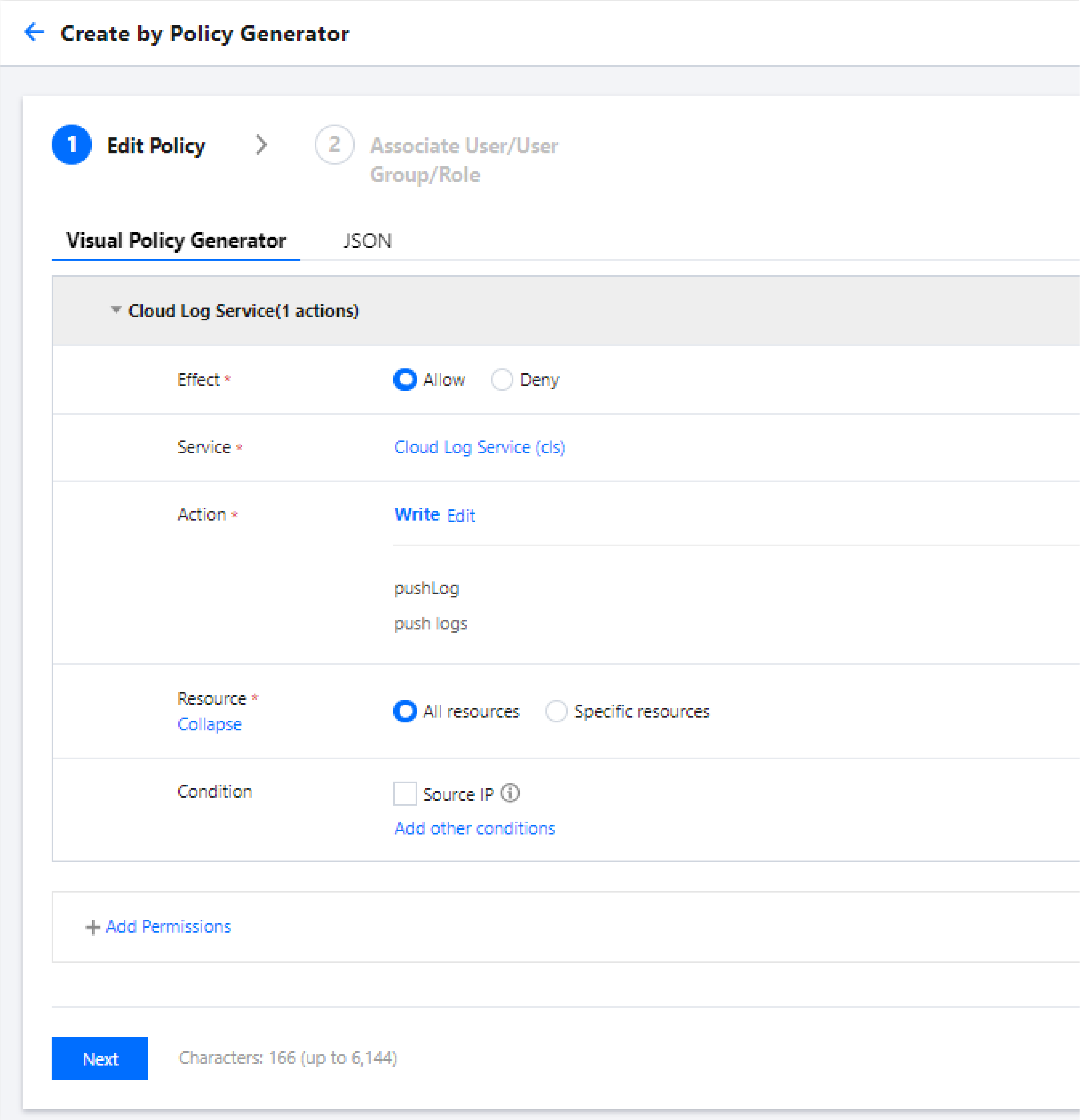
Example: Binding a service role to a container instance

Scenario example: Allowing container instances to upload logs to the Cloud Log Service.

1. Create a policy, role-tke-cls.

(1) Enter the Tencent Cloud Console, and navigate to the **Cloud Access Management** > Policies page.
(2) Click **Create Custom Policy**, and customize a policy role-tke-cls.
(3) Customize a policy that allows log uploads (Note: different policies can be assigned to roles in different scenarios).

©2013-2022 Tencent Cloud. All rights reserved.



Create by Policy Generator

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

Visual Policy Generator | JSON

Cloud Log Service(1 actions)

Effect * ● Allow ○ Deny

Service * Cloud Log Service (cls)

Action * Write Edit

pushLog
push logs

Resource * Collapse ● All resources ○ Specific resources

Condition □ Source IP ⓘ
Add other conditions

+ Add Permissions

Next Characters: 166 (up to 6,144)

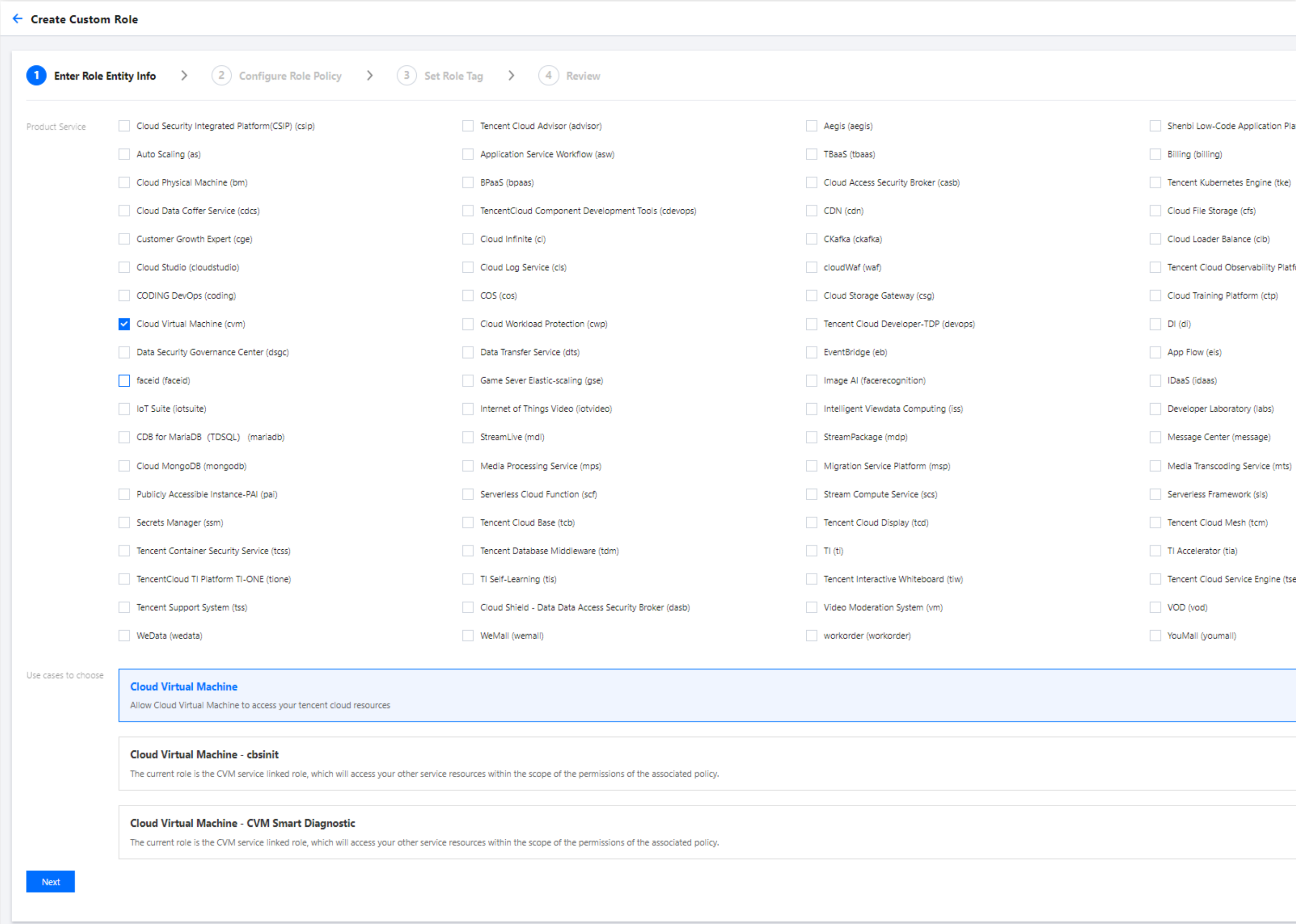
(4)The policy is created.

2. Create a role instance-role.

(1) Enter the Tencent Cloud Console, and navigate to the **Cloud Access Management** > Roles page.

(2) Click **Create Role**, and customize a role instance-role.

(3) Select **Cloud Server (CVM)** for the role carrier.



Create Custom Role

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

Product Service

□ Cloud Security Integrated Platform(CSIP) (csip)
□ Auto Scaling (as)
□ Cloud Physical Machine (bm)
□ Cloud Data Coffer Service (cdcs)
□ Customer Growth Expert (cge)
□ Cloud Studio (cloudstudio)
□ CODING DevOps (coding)
☑ Cloud Virtual Machine (cvm)
□ Data Security Governance Center (dsgc)
□ faceid (faceid)
□ IoT Suite (iotsuite)
□ CDB for MariaDB (TDSQL) (mariadb)
□ Cloud MongoDB (mongodb)
□ Publicly Accessible Instance-PAI (pai)
□ Secrets Manager (ssm)
□ Tencent Container Security Service (tcss)
□ TencentCloud TI Platform TI-ONE (tione)
□ Tencent Support System (tss)
□ WeData (wedata)
□ Tencent Cloud Advisor (advisor)
□ Application Service Workflow (asw)
□ BPaaS (bpaas)
□ TencentCloud Component Development Tools (cdevops)
□ Cloud Infinite (ci)
□ Cloud Log Service (cls)
□ COS (cos)
□ Cloud Workload Protection (cwp)
□ Data Transfer Service (dts)
□ Game Sever Elastic-scaling (gse)
□ Internet of Things Video (iotvideo)
□ StreamLive (mdl)
□ Media Processing Service (mps)
□ Serverless Cloud Function (scf)
□ Tencent Cloud Base (tcb)
□ Tencent Database Middleware (tdm)
□ TI Self-Learning (tis)
□ Cloud Shield - Data Data Access Security Broker (dasb)
□ WeMall (wemall)
□ Aegis (aegis)
□ TBaaS (tbaas)
□ Cloud Access Security Broker (casb)
□ CDN (cdn)
□ CKafka (ckafka)
□ cloudWaf (waf)
□ Cloud Storage Gateway (csg)
□ Tencent Cloud Developer-TDP (devops)
□ EventBridge (eb)
□ Image AI (facerecognition)
□ Intelligent Viewdata Computing (iss)
□ StreamPackage (mdp)
□ Migration Service Platform (msp)
□ Stream Compute Service (scs)
□ Tencent Cloud Display (tcd)
□ TI (ti)
□ Tencent Interactive Whiteboard (tiw)
□ Video Moderation System (vm)
□ workorder (workorder)
□ Shenbi Low-Code Application Pla
□ Billing (billing)
□ Tencent Kubernetes Engine (tke)
□ Cloud File Storage (cfs)
□ Cloud Loader Balance (clb)
□ Tencent Cloud Observability Platf
□ Cloud Training Platform (ctp)
□ DI (di)
□ App Flow (eis)
□ IDaaS (idaas)
□ Developer Laboratory (labs)
□ Message Center (message)
□ Media Transcoding Service (mts)
□ Serverless Framework (sls)
□ Tencent Cloud Mesh (tcm)
□ TI Accelerator (tia)
□ Tencent Cloud Service Engine (tse
□ VOD (vod)
□ YouMall (youmall)

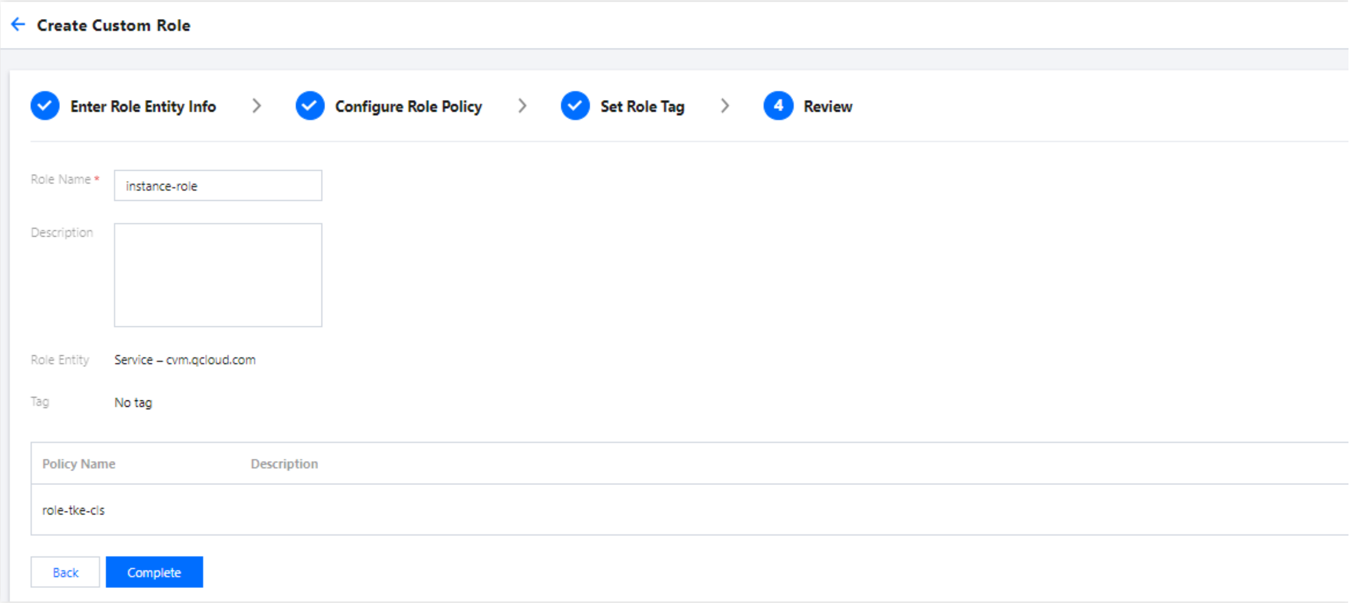
Use cases to choose

Cloud Virtual Machine
Allow Cloud Virtual Machine to access your tencent cloud resources

Cloud Virtual Machine - cbsinit
The current role is the CVM service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Cloud Virtual Machine - CVM Smart Diagnostic
The current role is the CVM service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

(4) The role is created.



Create Custom Role

✓ Enter Role Entity Info > ✓ Configure Role Policy > ✓ Set Role Tag > 4 Review

Role Name * instance-role

Description

Role Entity Service – cvm.qcloud.com

Tag No tag

Policy Name	Description
role-tke-cls	

3. Bind the role to the container instance.

(1) Enter the Tencent Cloud Console, and navigate to the Container Instance List page.

(2) Click **New Instance**. Set the container instance parameters based on your actual requirements.

(3) Select the pre-created role instance-role for the CAM role, and complete the binding.

©2013-2022 Tencent Cloud. All rights reserved.

Other Resource-based Service Roles

If you need to bind roles to your Tencent Kubernetes Engine - Container Instances, please refer to Binding a Role to a Container Instance.

If you need to bind roles to your Serverless Cloud Function - Function Service, please refer to Role and Authorization.

If you need to bind roles to your Cloud Server - Cloud Hosts, please refer to Managing Roles.

©2013-2022 Tencent Cloud. All rights reserved.

Policies

Concepts

Last updated：2024-01-23 17:54:33

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.

A policy is a syntax rule used to define and describe one or more permissions. CAM supports two types of policies: preset policies and custom policies. Preset policies are common permission sets created and managed by Tencent Cloud, such as super admin and cloud resource admin. These are read-only and cannot be edited. Custom policies are user-defined permission sets that describe resource management with a finer granularity. The former cannot specifically describe individual resources and has a coarser granularity, while the latter can flexibly meet differentiated permission management needs.

A user or user group can be associated with one or multiple policies for authorization. The authorized policy can either be a preset or custom.

Definition

Policy

Last updated：2024-01-23 17:54:33

A policy is a syntax rule used to define and describe one or more permissions. CAM supports two types of policies: preset policies and custom policies. It offers multiple ways to create and manage policies from different perspectives. If you need to add permissions to a CAM user or group, you can directly associate a preset policy or create a custom policy for association. Each policy can contain multiple permissions, and you can also choose to bind multiple policies to one CAM user or group.

Preset Policy

Preset policies are common permission sets created and managed by Tencent Cloud that are frequently used by users, such as super admin and full resource access. Preset policies cover a wide range of operation objects at a coarse operation granularity. They are preset by the system and cannot be edited by users.

Custom Policy

Custom policies are user-defined permission sets that describe resource management with finer granularity. It allows fine-grained permission division and can flexibly meet your differentiated permission management needs. For example, you can associate a policy with a database admin so that the admin has the permissions to manage TencentDB instances but not CVM instances.

©2013-2022 Tencent Cloud. All rights reserved.

Authorization Guide
Creating Custom Policy

Last updated：2024-01-23 17:54:33

Overview

This document describes how to create a custom policy in different ways. A custom policy allows granular permission division and can flexibly meet your differentiated permission management needs.

Directions

Creating by policy generator

With a policy created by the policy generator, you can create policy syntax automatically by selecting services and actions (operations) and defining resources. This method is highly recommended for its simplicity and flexibility.
1. On the Policy page in the CAM console, click **Create Custom Policy** in the top-left corner.
2. In the selection window that pops up, click **Create by Policy Generator** to enter the **Edit Policy** page.
3. Select the service in the **Visual Policy Generator**, enter the following information, and edit an authorization statement. (You can also choose JSON to use the policy syntax method to edit the policy, and the authorization effect is the same as the **Visual Policy Generator**).
Effect (required): select **Allow** or **Deny**.
Service (required): select the service you want to authorize.
Action (required): select the operations you want to authorize.
Resource (required): select all resources or specific resources you want to authorize.
Tencent Cloud products with operation-level or service-level authorization granularity do not support six-segment resource descriptions. For such products, simply select all resources.
For Tencent Cloud products with resource-level authorization granularity, you can select specific resources. For more information on the resource description method, please see the corresponding CAM Guide in CAM-Enabled Products.
For more information on the authorization granularities of Tencent Cloud products, please see the Authorization Granularity section in CAM-Enabled Products.
Condition (optional): set the conditions that must be met for the authorization to take effect. For more information, please see Condition.
Note:
If you want to authorize multiple services, you can click **Add Permission** to add multiple authorization statements and configure authorization policies for other services.

Multiple statements can be added in one policy.

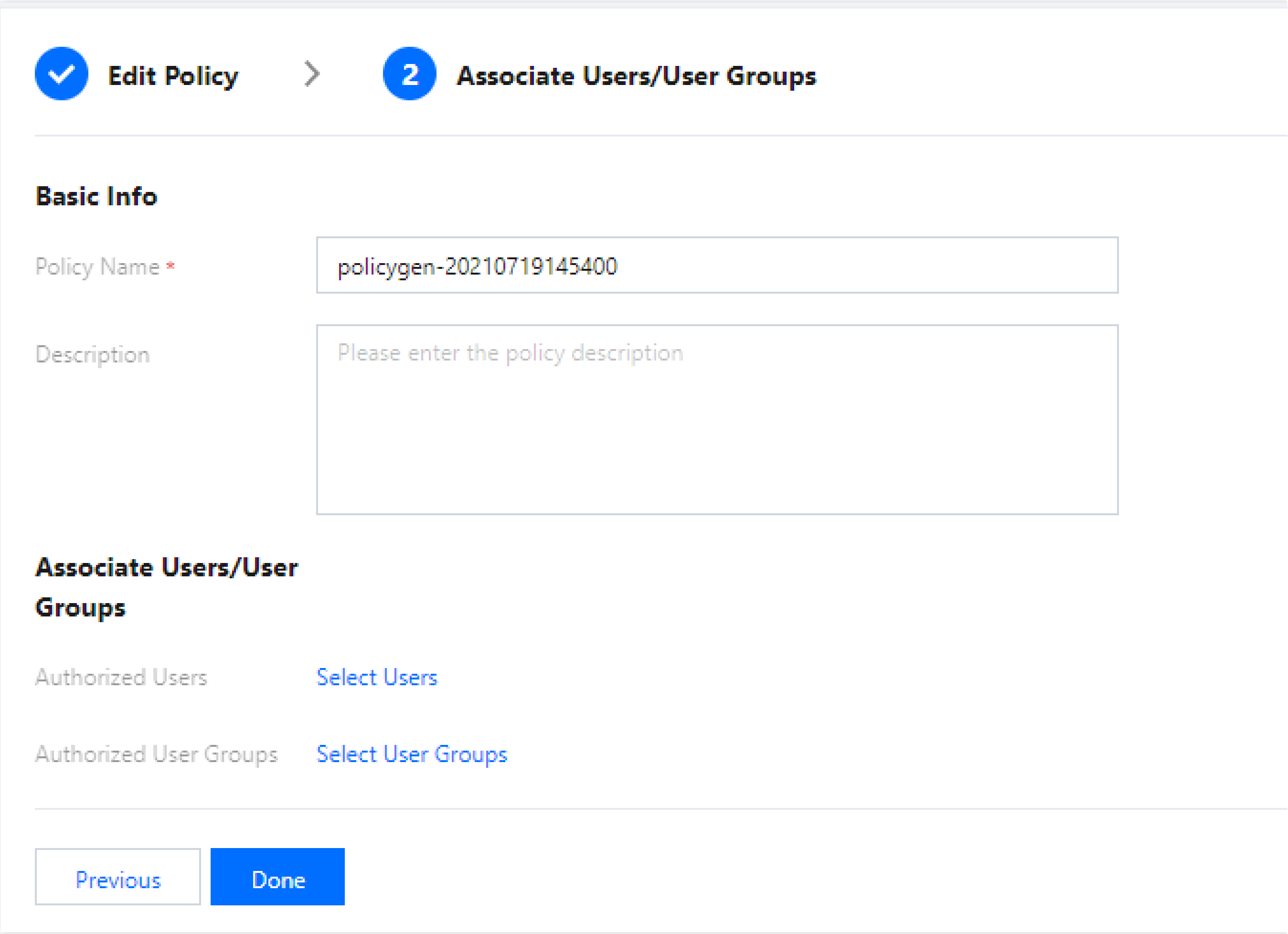
4. After editing the policy authorization statement, click **Next** to enter the **Associate with User/User Group** page.

5. On the **Associate with User/User Group** page, add the policy name and description, and you can associate users or user groups for quick authorization at the same time.

Note:

The policy name is automatically generated by the console and is `policygen` suffixed with the creation time by default, which is customizable.

6. Click **Done** to complete the custom policy creation.



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：2024-01-23 17:54:33

Overview

This document describes the process of creating customized policies through tag authorization. After the policy is generated, it will possess the authority over a category of tag attribute resources. For definitions related to the policy, please refer to Concepts.

Directions

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 involves 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, which will include operation permissions for resources associated with corresponding tags.

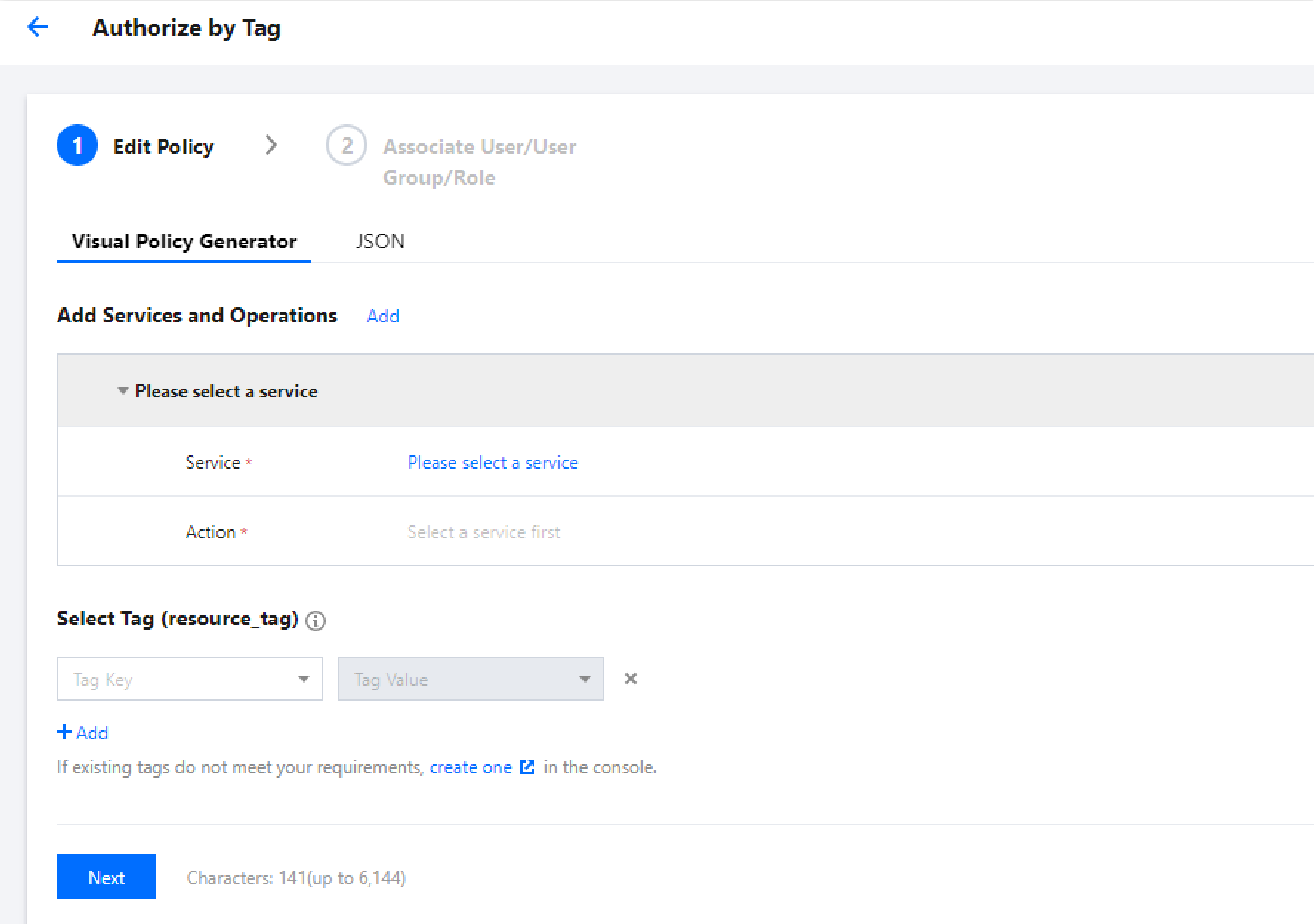
No: Does not support tag-based authorization, which will include operation permissions for all resources.

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 to 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.

©2013-2022 Tencent Cloud. All rights reserved.



Authorize by Tag

Add Services and Operations Add

Please select a service

Service * Please select a service

Action * Select a service first

Select Tag (resource_tag)

If existing tags do not meet your requirements, create one in the console.

Characters: 141(up to 6,144)

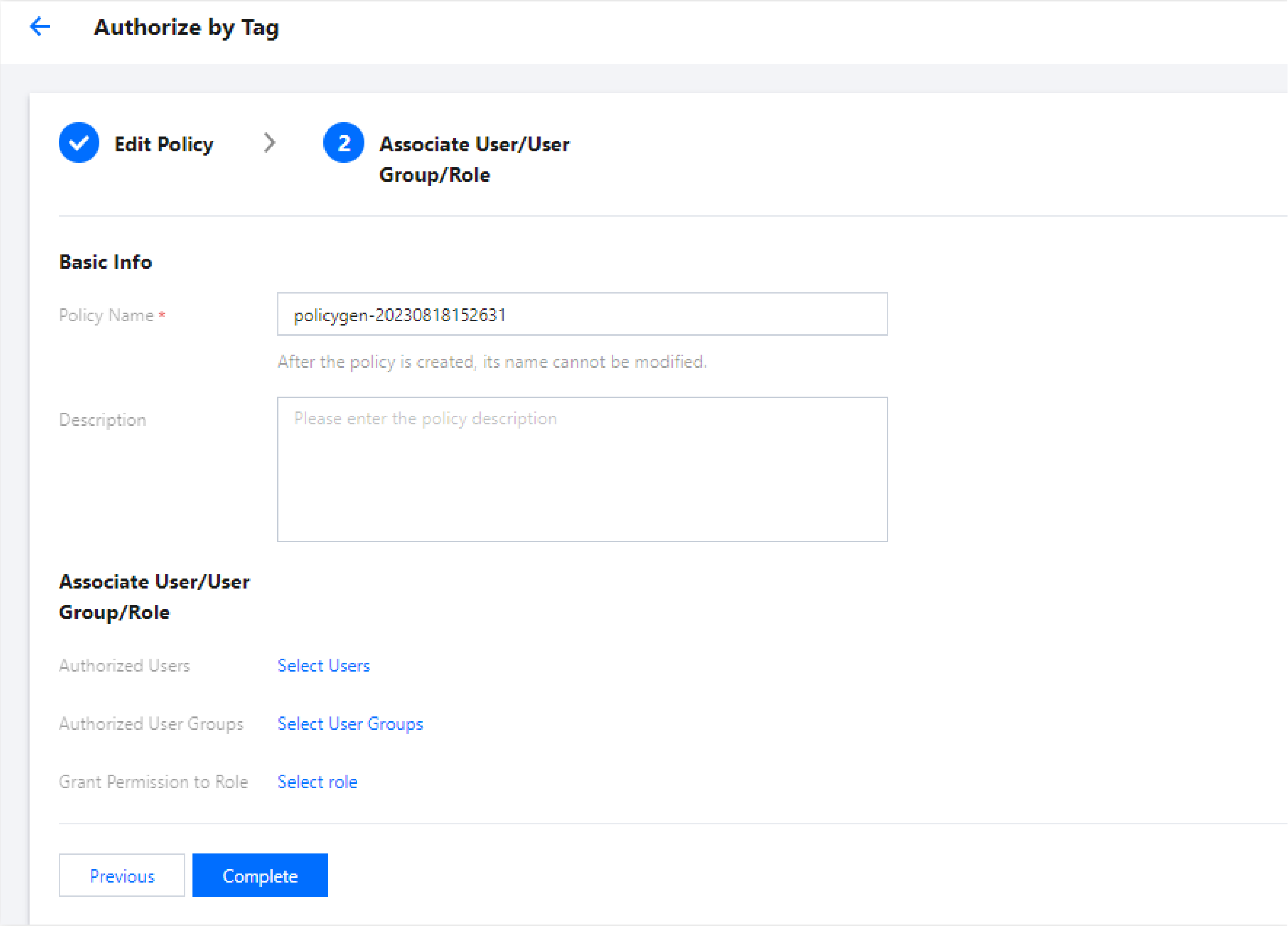
5. On the Associate User/User Group/Role page, enter the policy name and description information. You can also associate users/user groups/roles for quick authorization.

Note

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

6. Click **Complete** to finish creating the customized policy.

©2013-2022 Tencent Cloud. All rights reserved.



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

Subsequent Procedures

Authorization Management

©2013-2022 Tencent Cloud. All rights reserved.

Creating Custom Policies through Policy Syntax

Last updated：2024-01-23 17:54:33

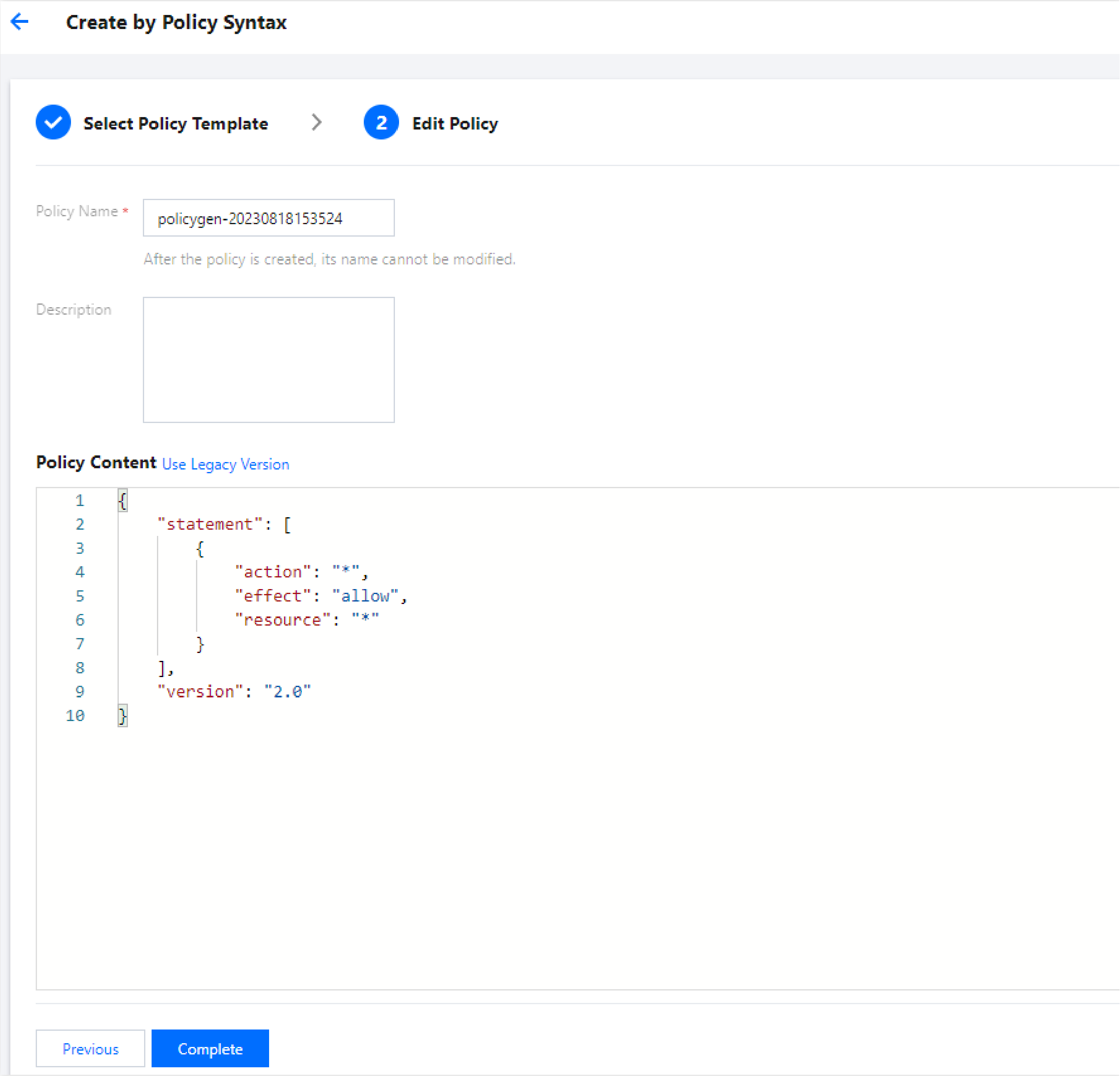
Overview

This document describes the process of creating customized policies through policy syntax, a method that involves the user crafting the policy syntax to generate corresponding policies. This approach offers flexible permission granularity, effectively meeting the demands of users who require a meticulous delineation of permissions. For definitions related to policies, please refer to Concepts.

Directions

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, you can enter the keyword 'a' to 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 finish creating the customized policy. The default policy name and policy content are automatically generated by the console. The default policy name is **policygen**, with a suffix number generated according to the creation date.

©2013-2022 Tencent Cloud. All rights reserved.



Policy Name * policygen-20230818153524

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

Description

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

Subsequent Procedures

Authorization Management

Authorization Management

Last updated：2024-01-23 17:54:33

Overview

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.

Prerequisites

You have created a sub-user or user group.

If you need to associate a custom policy, please create one first.

Directions

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 policy with user

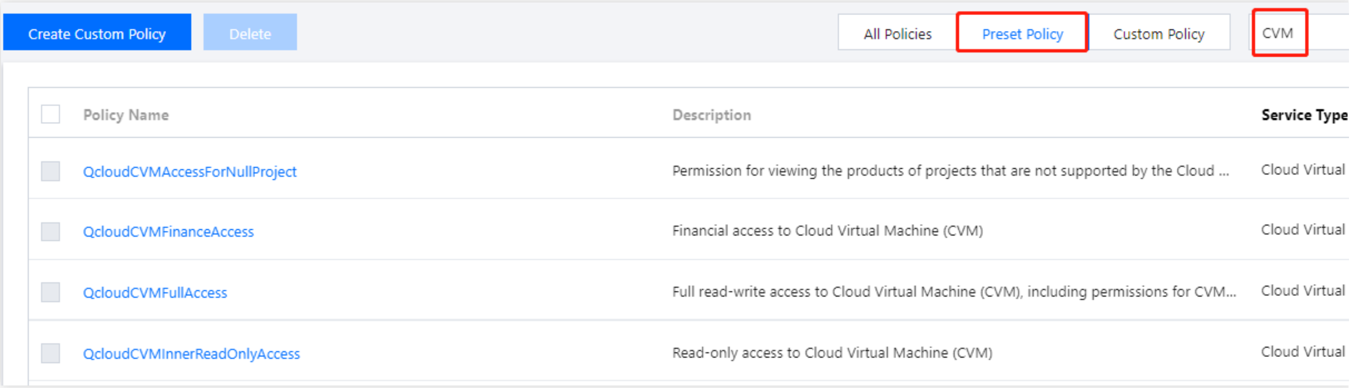
Associating policy with user group

1. On the **Policies** page in the CAM console, select a policy type.

Note:

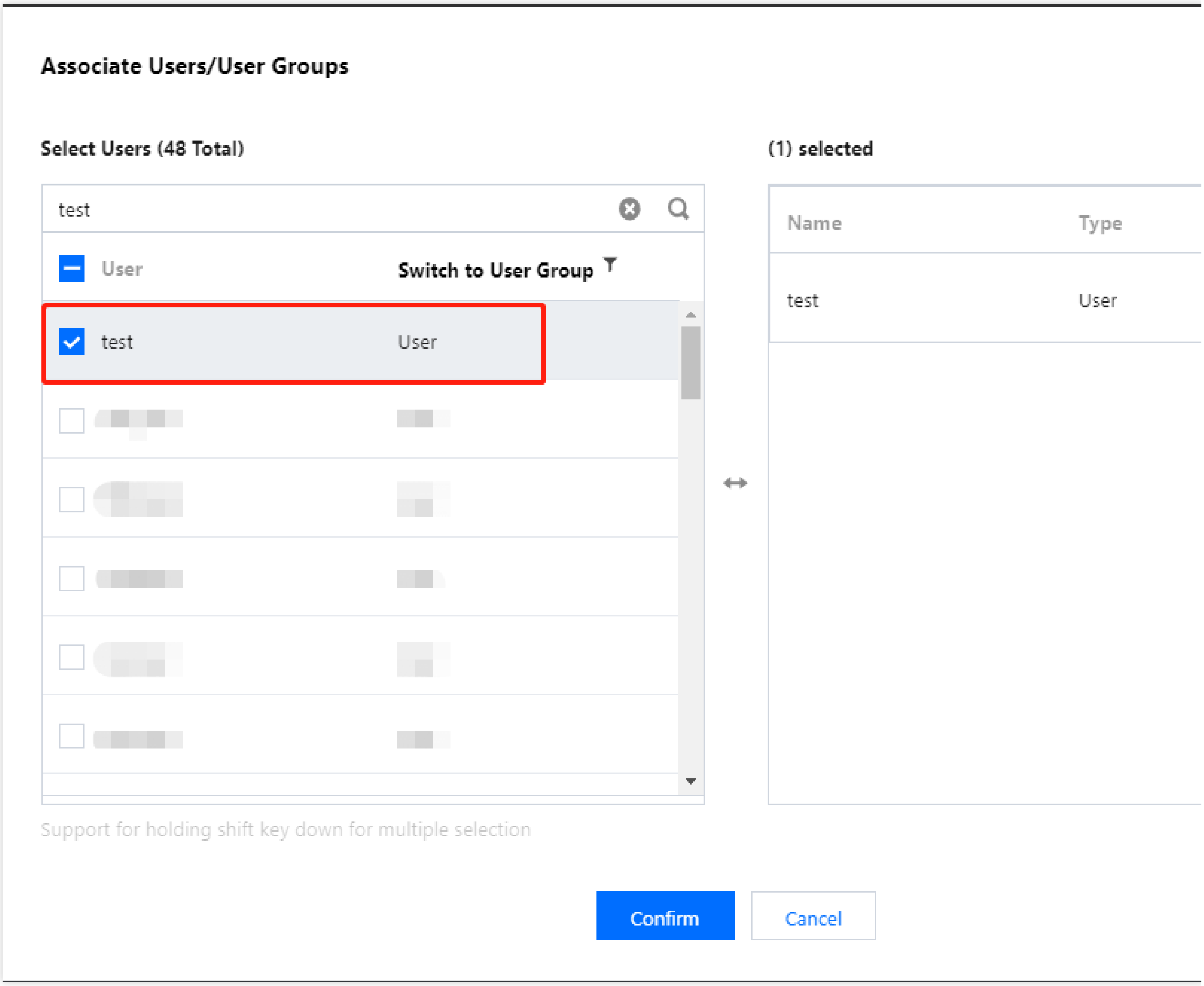
This document takes a **preset policy** as an example. You can also select a **custom policy**.

2. Search for the preset policy you want to associate and click **Associate Users/Groups** in the **Operation** column.



Policy Name	Description	Service Type
QcloudCVMAccessForNullProject	Permission for viewing the products of projects that are not supported by the Cloud ...	Cloud Virtual
QcloudCVMFinanceAccess	Financial access to Cloud Virtual Machine (CVM)	Cloud Virtual
QcloudCVMFullAccess	Full read-write access to Cloud Virtual Machine (CVM), including permissions for CVM...	Cloud Virtual
QcloudCVMInnerReadOnlyAccess	Read-only access to Cloud Virtual Machine (CVM)	Cloud Virtual

3. In the **Associate Users/User Groups** pop-up window, select the user you want to associate and click **OK** to complete the association.



Associate Users/User Groups

Select Users (48 Total)

test

User	Switch to User Group
☑ test	User

(1) selected

Name	Type
test	User

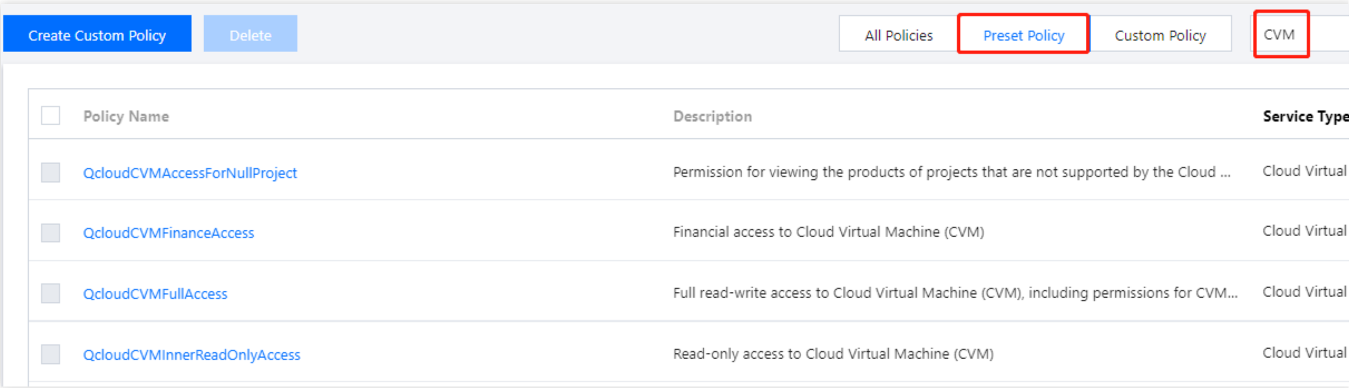
Support for holding shift key down for multiple selection

1. On the **Policies** page in the CAM console, select a policy type.

Note:

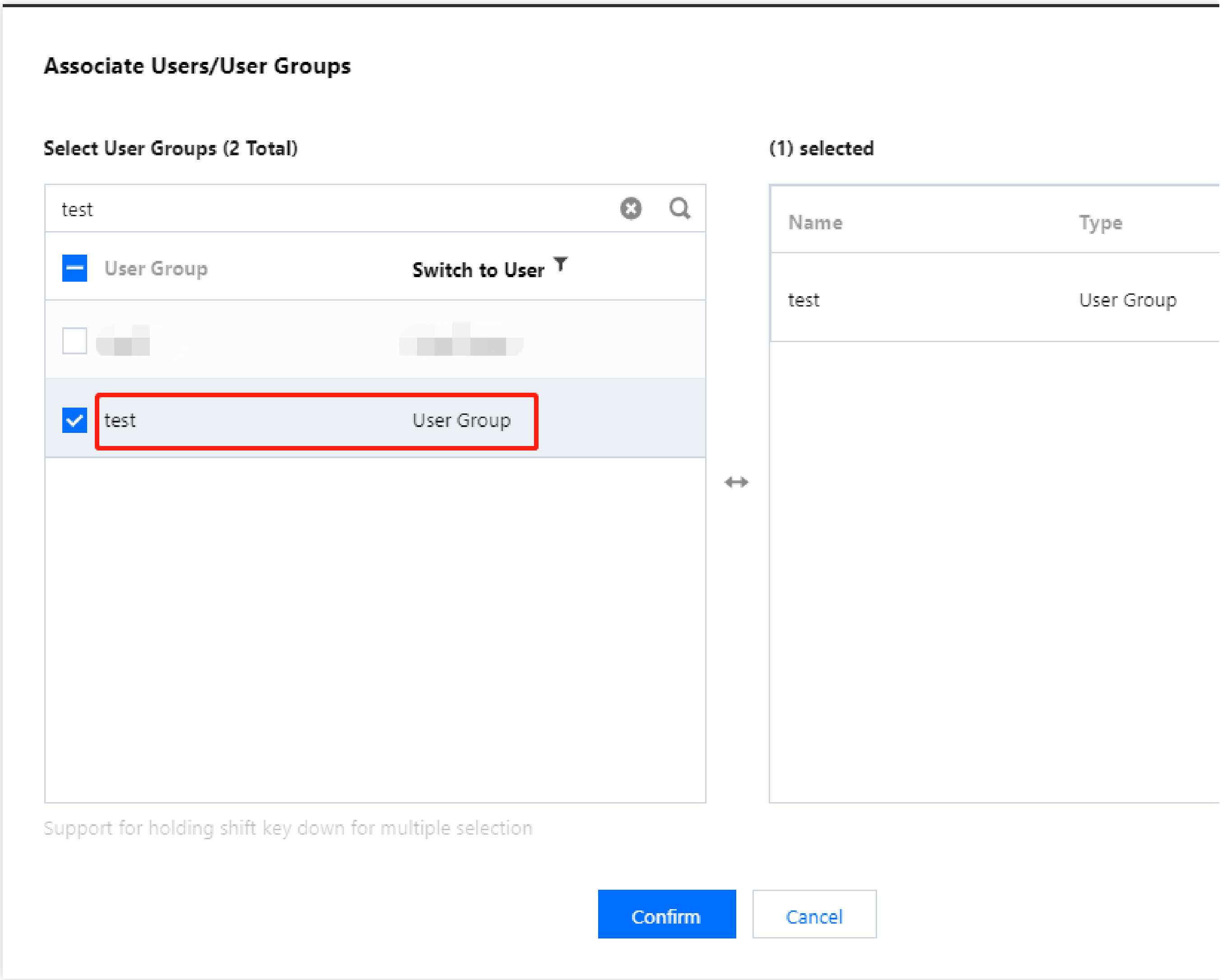
This document takes a **preset policy** as an example. You can also select a **custom policy**.

2. Search for the preset policy you want to associate and click **Associate Users/Groups** in the **Operation** column.



Policy Name	Description	Service Type
QcloudCVMAccessForNullProject	Permission for viewing the products of projects that are not supported by the Cloud ...	Cloud Virtual
QcloudCVMFinanceAccess	Financial access to Cloud Virtual Machine (CVM)	Cloud Virtual
QcloudCVMFullAccess	Full read-write access to Cloud Virtual Machine (CVM), including permissions for CVM...	Cloud Virtual
QcloudCVMInnerReadOnlyAccess	Read-only access to Cloud Virtual Machine (CVM)	Cloud Virtual

3. In the **Associate Users/User Groups** pop-up window, click **Switch to User Group**.
4. Select the user group you want to associate and click **OK** to complete the association.

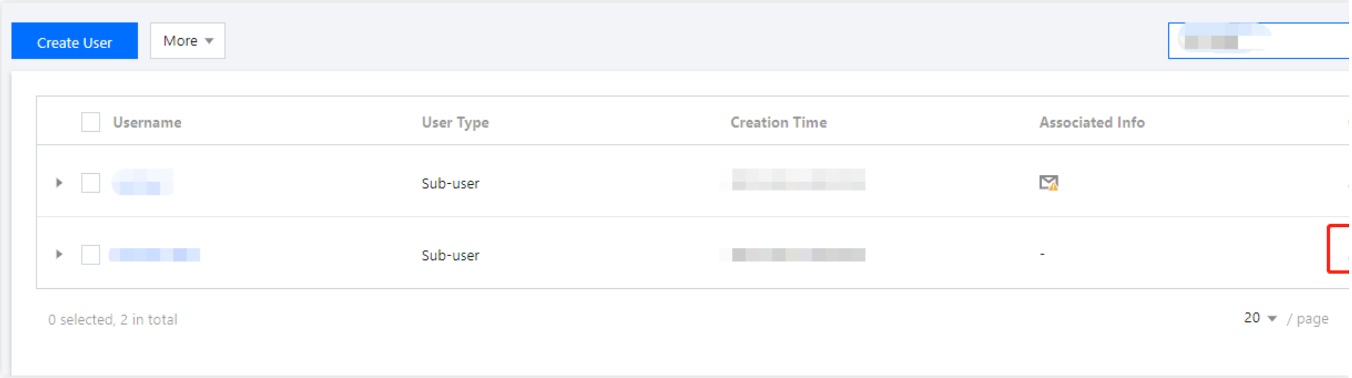

Associate Users/User Groups
Select User Groups (2 Total)
test
User Group
Switch to User
test
User Group
(1) selected
Name
Type
test
User Group
Support for holding shift key down for multiple selection
Confirm
Cancel

Associating user/user group with policy

Associating user with policy

Associating user group with policy

1. On the **Users** > **User List** page in the CAM console, find the user to be authorized and click **Authorization** in the **Operation** column to enter the **Associate Policy** page.



	Username	User Type	Creation Time	Associated Info
□	[redacted]	Sub-user	[redacted]	✉
□	[redacted]	Sub-user	[redacted]	-

0 selected, 2 in total

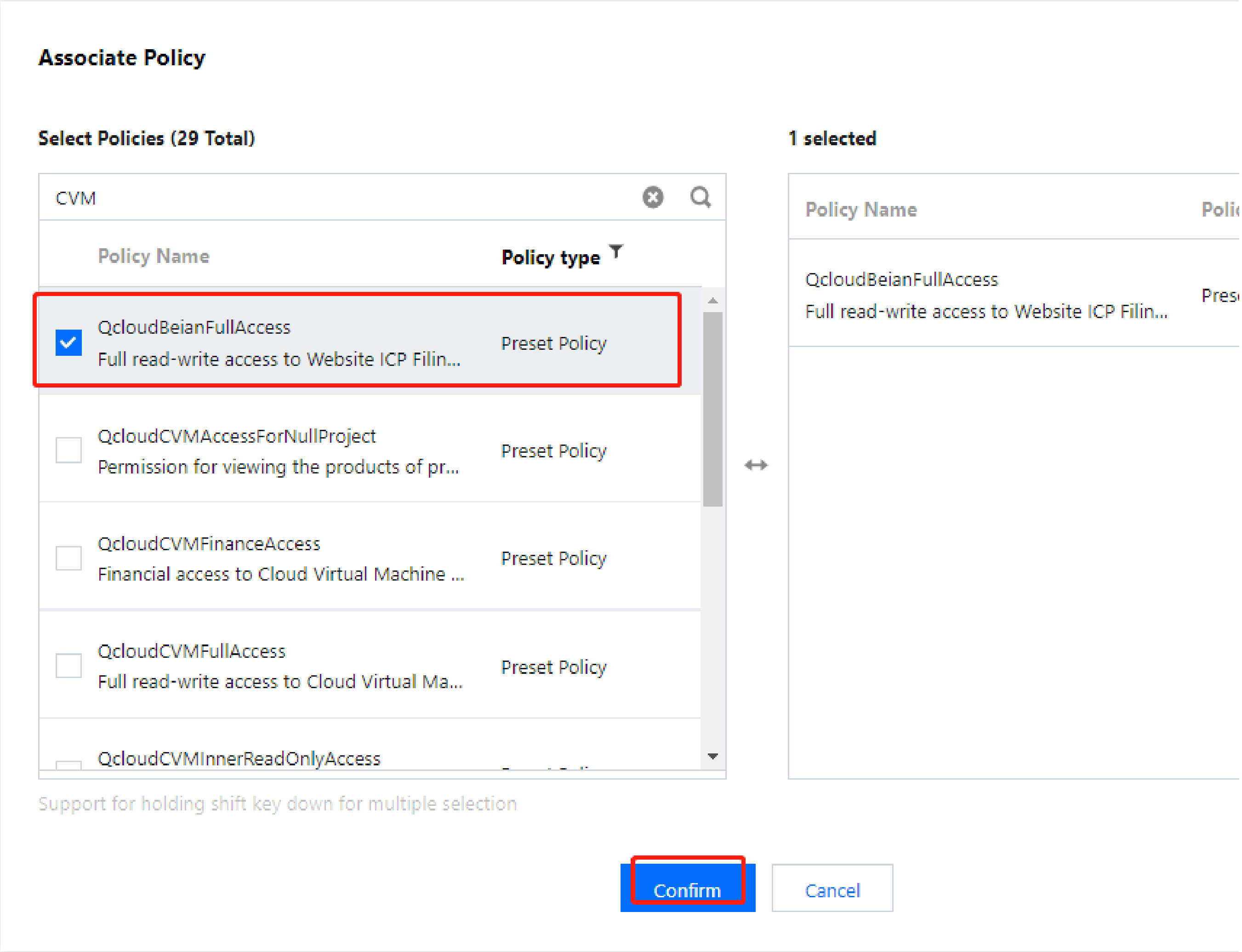
20 / page

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 you want to associate and click **OK** to complete the association.



Associate Policy

Select Policies (29 Total)

CVM

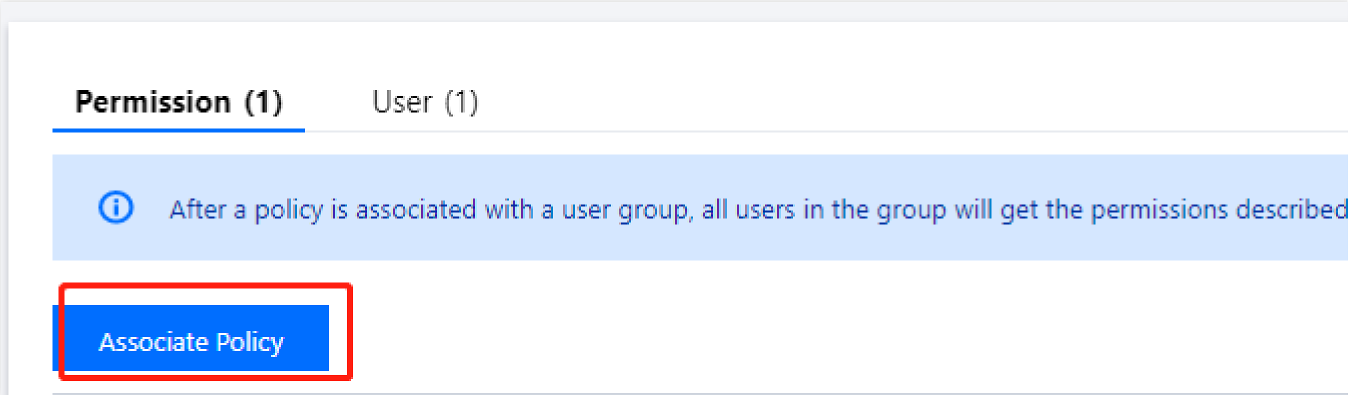
	Policy Name	Policy type
☑	QcloudBeianFullAccess Full read-write access to Website ICP Filin...	Preset Policy
□	QcloudCVMAccessForNullProject Permission for viewing the products of pr...	Preset Policy
□	QcloudCVMFinanceAccess Financial access to Cloud Virtual Machine ...	Preset Policy
□	QcloudCVMFullAccess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

Support for holding shift key down for multiple selection

1 selected

Policy Name	Poli
QcloudBeianFullAccess Full read-write access to Website ICP Filin...	Pres

1. On the **User Groups** page in the CAM console, click the name of the target user group to enter the user group details page.
2. On the user group details page, click **Associate Policy** to enter the **Associate Policy** page.



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

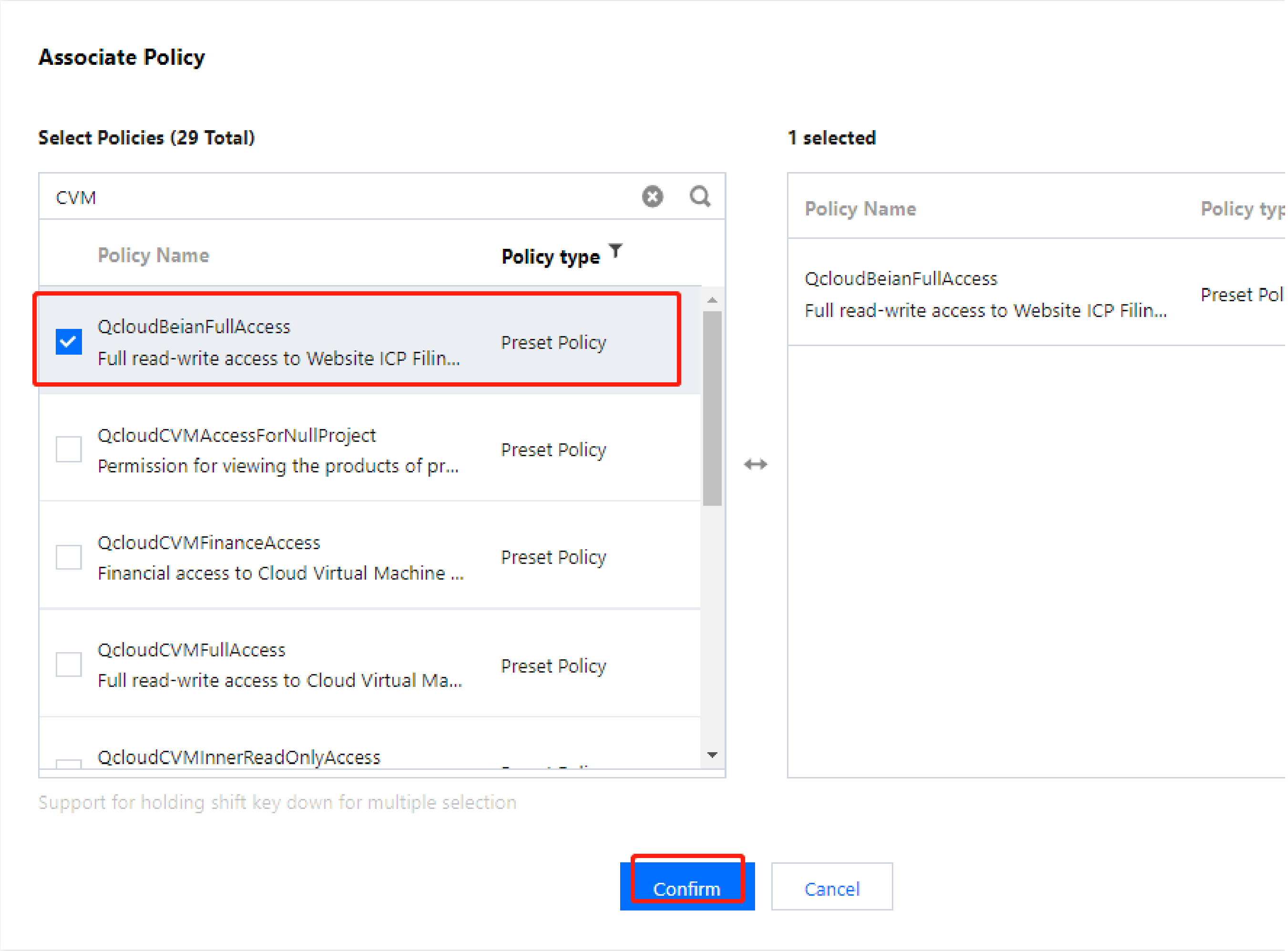
3. On the **Associate Policy** page, select a policy type.

Note:

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

©2013-2022 Tencent Cloud. All rights reserved.

4. Select the policy you want to associate and click **OK** to complete the association.



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 typ
QcloudBeianFullAccess Full read-write access to Website ICP Filin...	Preset Pol

Relevant Documents

For more information on the concept of policy, please see Policy.

©2013-2022 Tencent Cloud. All rights reserved.

IP Access Restrictions

Last updated：2024-01-23 17:54:33

Introduction

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.

Prerequisites

The product must support limiting access via IP. For more information, see FAQs.

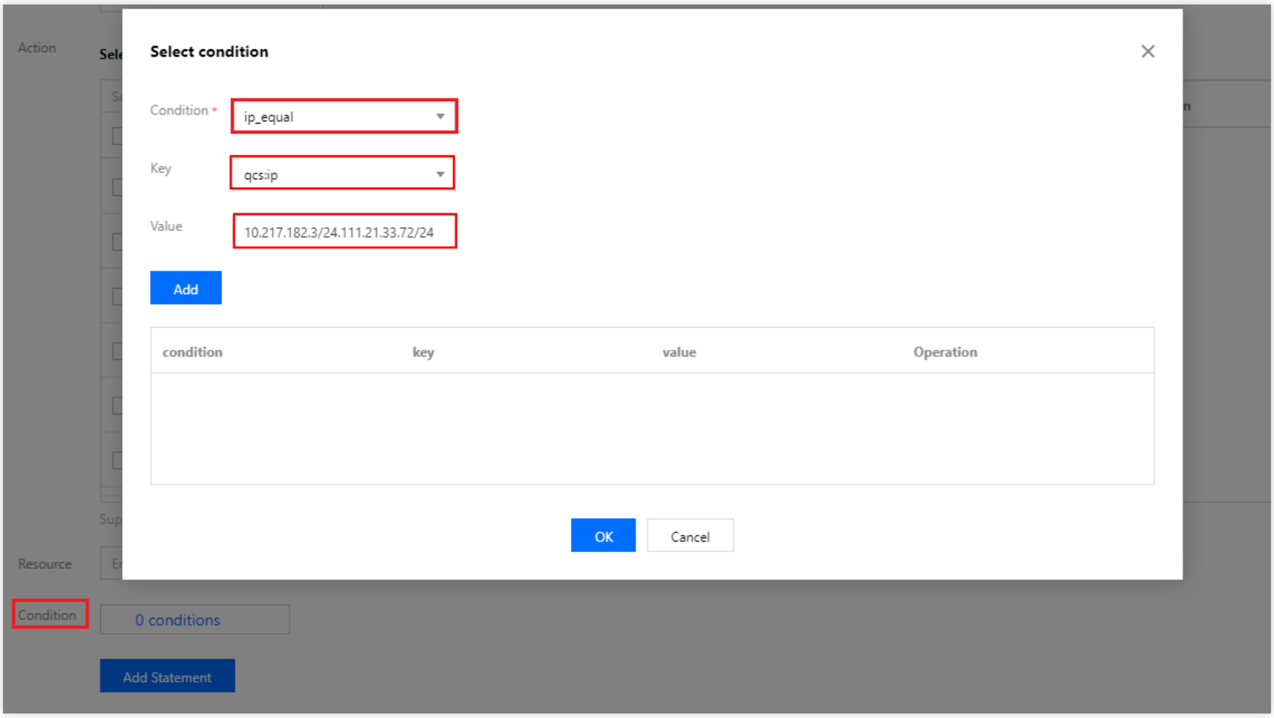
Directions

1. Go to the Policies management page and click **New Custom Policy** in the upper left corner.
2. In the selection window that pops up, click **Create by Policy Generator**.
3. In the Service and Action selection page, enter the following information:

Effect: Required. Select “Allow”. If you choose “Deny”, users or groups will not be able to obtain authorization.
Service: Required. Select the product you want to add.
Action: Required. Select product permissions according to your requirements.
Resources: Required. For more information on what to enter, see Resource Description Method.
Conditions: Enter the IP address according to your needs. You can add multiple restrictions. For example, for effect, select **Allow** to only permit users or groups from this IP address to obtain authorization.

Use Case

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:



Condition * ip_equal

Key qcs:ip

Value 10.217.182.3/24.111.21.33.72/24

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

Element Reference Overview

Last updated：2024-06-27 16:14:52

A policy is made up of elements that describe specific information of the authorization. Core elements include `principal` , `action` , `resource` , `condition` , and `effect` . These elements must be lowercase. The order of the elements does not matter. The `condition` element is optional. The `principal` element cannot be used in the console and can only be used through policy management APIs and policy syntax-related parameters.

1. version

This required element defines the version of policy syntax. At present, the only available value is "2.0".

2. principal

This element specifies the entity to be authorized by the policy. This includes users (root accounts and sub-accounts). In the future, more entities will be included, such as roles and federated users. This element can only be used in trust policies for roles and COS bucket policies.

3. statement

This element describes the details of one or more permissions. It contains a permission or permission set of multiple other elements such as `action` , `resource` , `condition` , and `effect` . One policy has only one `statement` .

4. action

This required element describes the action (operation) to be allowed or denied. An operation can be an API (prefixed with `name`) or a feature set (a set of specific APIs prefixed with `actionName`).

5. resource

This required element describes the objects the statement covers. A resource is described in a six-segment format. Detailed resource definitions vary by product. For more information on how to specify a resource, please see the documentation for the product whose resources you are writing a statement for.

6. condition

This optional element describes the condition for the policy to take effect. A condition consists of operator, action key, and action value. A condition value may contain information such as time and IP address. Some services allow you to specify additional values in a condition.

7. effect

This required element describes whether the statement result is an "allow" or "explicit deny".

8. Sample policy

The following sample policy grants a sub-account (ID: 3232523) of a root account (APPID: 1238423) permissions to use all COS read APIs, write objects, and send message queues for the COS bucket "bucketA" in the Beijing region and the COS object "object2" in the bucket "bucketB" in the Guangzhou region when the access IP falls within the IP range of `10.121.2.*` .

©2013-2022 Tencent Cloud. All rights reserved.

```
{
  "version": "2.0",
  "statement": [
    {
      "principal": {
        "qcs": [
          "qcs::cam::uin/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::uin/1238423:uin/3232523"
        ]
      },
      "effect": "allow",
      "action": "cmqqueue:SendMessage",
      "resource": "*"
    }
  ]
}
```

Relevant documents

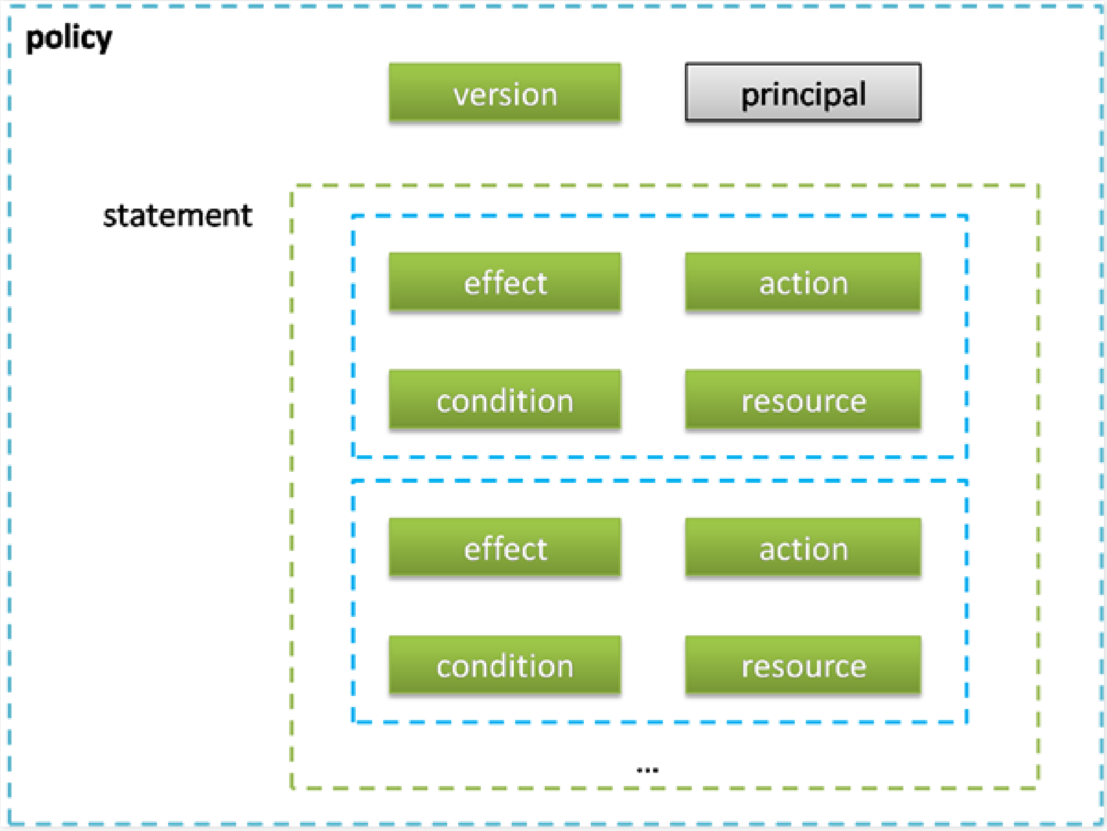
For more information on `resource` in CAM, please see Resource Description Method.

Syntax Structure

Last updated：2024-01-23 17:56:33

The syntax structure of a policy is as shown in the following figure. The policy consists of a `version` and a `statement`, and can also contain `principal` information. `principal` can only be used in policy syntax-related parameters in policy management APIs.

A `statement` is composed of several sub-statements. Each sub-statement contains four elements: `action`, `resource`, `condition`, and `effect`, where `condition` is optional.



JSON Format

The policy syntax is based on the JSON format as defined in RFC 7159. If a created or updated policy does not meet the JSON format requirement, it cannot be successfully submitted. Therefore, you must ensure that the JSON format is correct. You can check the policy format with an online JSON validator.

Syntax Conventions

Here we list some syntax conventions:

These characters are JSON characters included in policy syntax:

©2013-2022 Tencent Cloud. All rights reserved.

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

These characters are special characters used to describe policy syntax and are not included in policies:

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

If an element allows multiple values, the values will be described with comma separators and ellipsis; for example:

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

When multiple values are allowed, you can also choose to include only one value. When an element has only one value, the trailing comma must be removed, and the brackets "[]" are optional; for example:

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

The question mark "?" behind an element indicates that the element is optional; for example:

```
<condition_block?>
```

If an element is enumerated, use vertical line "|" to separate the values and use parenthesis "()" to define the range of the enumerated values; for example:

©2013-2022 Tencent Cloud. All rights reserved.

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

String elements are enclosed in double quotation marks; for example:

```
<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> = {
```

©2013-2022 Tencent Cloud. All rights reserved.

```
    <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:

One policy may contain multiple `statement` .

The maximum length of a policy is 6144 characters (without spaces). For more information, please see Limits.

The display order of blocks is unrestricted; for example, in a policy, `version_block` can follow `effect_block` .

Currently supported syntax version is 2.0.

The `principal_block` element cannot be used in the console and can only be used through policy management APIs and policy syntax-related parameters.

Lists are supported for both `action` and `resource` .

A condition can be a single condition or a logical combination of multiple sub-conditions. Each condition contains a condition operator `condition_type` , a condition key `condition_key` , and a condition value `condition_value` .

The `effect` of each statement is `deny` or `allow` . If the statement of a policy contains both `allow` and `deny` , `deny` will take 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 operations for 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 C
"action":["cos:GetBucketPolicy","cos:PutBucketPolicy","cos: DeleteBucketPolicy"]
```

resource_string

Resource is described in a six-segment format.

©2013-2022 Tencent Cloud. All rights reserved.

```
qcs: project :serviceType:region:account:resource
```

Below are examples:

```
// COS object. Region: Shanghai. Resource owner uid: 10001234. Resource name: bucke
qcs::cos:sh:uid/10001234:prefix//10001234/bucket1/object2
// CMQ queue. Region: Shanghai. Resource owner uin: 12345678. Resource name: 123456
qcs::cmqqueue:sh:uin/12345678:queueName/12345678/queueName1
// CVM instance. Region: Shanghai. Resource owner uin: 12345678. Resource name: ins
qcs::cvm:sh:uin/12345678:instance/ins-abcdefg
```

For more information on product-specific resource definitions, please see the corresponding product documentation in CAM-Enabled Tencent Cloud Products.

condition_type_string

Condition operator describes the type of test conditions, such as `string_equal` , `string_not_equal` , `date_equal` , `date_not_equal` , `ip_equal` , `ip_not_equal` , `numeric_equal` , and `numeric_not_equal` . Below are examples:

```
"condition":{
          "string_equal":{"cvm:region":["sh","gz"]},
          "ip_equal":{"qcs:ip":"10.131.12.12/24"}
}
```

condition_key_string

Condition keys are used with a condition operator to determine whether the condition is met. CAM defines a set of condition keys that can be used in all products, including `qcs:current_time` , `qcs:ip` , `qcs:uin` , `qcs:owner_uin` , etc. For more information, please see Condition.

principal_id_string

For CAM, users are also its resources. Therefore, the `principal` also uses a six-segment description. Below is an example. For more information, please see Resource Description Method.

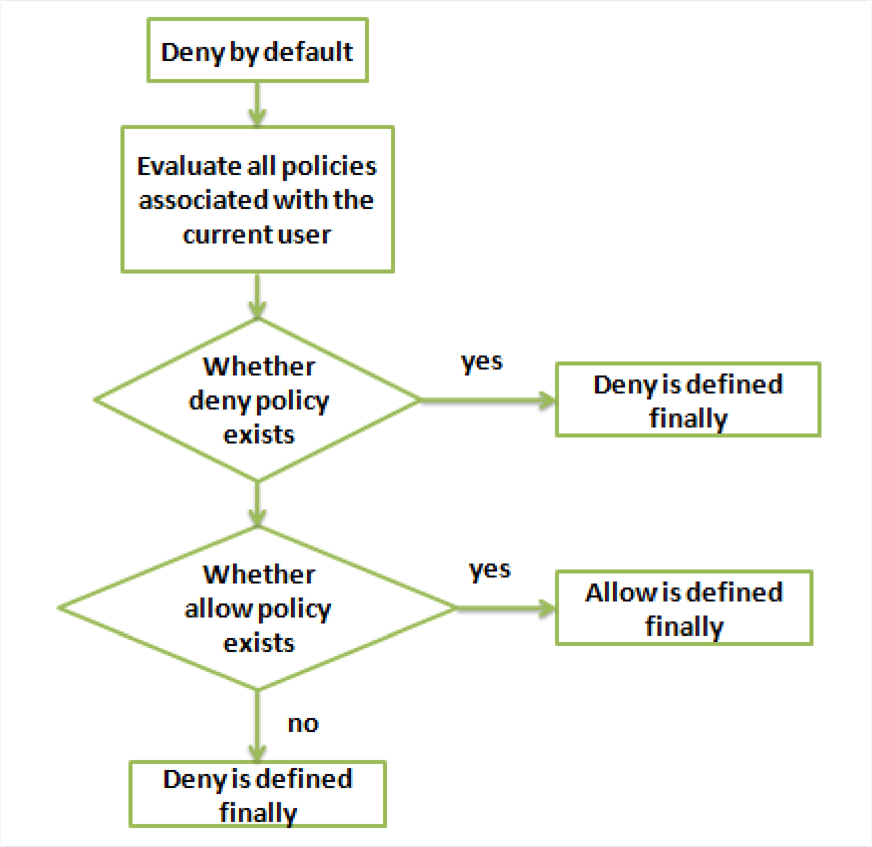
```
"principal":   {"qcs":["qcs::cam::uin/1238423:uin/3232",
                 "qcs::cam::uin/1238423:groupid/13"]}
```

©2013-2022 Tencent Cloud. All rights reserved.

Evaluation Logic

Last updated：2024-01-23 17:54:33

When a Tencent Cloud user accesses Tencent 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 deny policy exists
yes
Deny is defined finally
Whether allow policy exists
yes
Allow is defined finally
no
Deny is defined finally

1. All requests will be denied by default.
2. CAM will check all the policies currently associated with the user.
1. It will determine whether any policies match, and if so, it will proceed to the next step. If not, the final result is "deny", and access to Tencent Cloud resources is not permitted.
2. It will determine whether any "deny" policies match, and if so, the final result will be "deny", and access to Tencent Cloud resources is not permitted. If not, it will proceed to the next step.
3. It will determine whether any "allow" policies match, and if so, the final result will be "allow", and access to Tencent Cloud resources will be permitted. If not, the final result is "deny", and access to Tencent Cloud resources is not permitted.

Note：

©2013-2022 Tencent Cloud. All rights reserved.

A root account has full access to all resources it owns by default. At present, cross-account resource access is only supported for COS.

There are some general policies that are associated with all CAM users by default. For more information, please see the General Policy Table below.

Other policies need to be explicitly specified. This applies to both allow and deny policies.

For services that support cross-account resource access, permission propagation applies. For example, if root account A grants a sub-account under root account B access to its resources, CAM will verify whether root account A has granted root account B access and whether root account B has granted the sub-account access. Both must be true for the sub-account of root account B to be allowed to access root account A's resources.A root account has full access to all resources it owns by default. At present, cross-account resource access is only supported for COS.

The followin

g table lis

ts currently supported general policies:

Policy Description	Policy Definition

MFA verification is required for querying keys	{
	"principal":"*",
	"action":"account:QueryKeyBySecretId",
	"resource":"*",
	"condition":{"string_equal":{"mfa":"0"}}
	}

MFA verification is required for sensitive configurations	{
	"principal":"*",
	"action":"account:SetSafeAuthFlag",
	"resource":"*",
	"condition":{"string_equal":{"mfa":"0"}}
	}

MFA verification is required for binding tokens	{
	"principal":"*",
	"action":"account:BindToken",
	"resource":"*",
	"condition":{"string_equal":{"mfa":"0"}}
	}

MFA verification is required for unbinding tokens	{
	"principal":"*",
	"action":"account:UnbindToken",
	"resource":"*",
	"condition":{"string_equal":{"mfa":"0"}}
	}

MFA verification is required for modifying email addresses	{
	"principal":"*",
	"action":"account:ModifyMail",
	"resource":""",
	"condition":{"string_equal":{"mfa":"0"}}
	}

MFA verification is required for modifying mobile numbers	{
	"principal":"*",
	"action":"account:ModifyPhoneNum",
	"resource":""",
	"condition":{"string_equal":{"mfa":"0"}}
	}

©2013-2022 Tencent Cloud. All rights reserved.

Resource Description Method

Last updated：2024-01-23 17:54:33

The `resource` element describes one or multiple operation objects such as CVM resources and COS buckets. This document describes the resource information in CAM.

Definition of All Resources

If `resource` is `*`, it indicates all resources; that is, you can grant the `action` (operation) permission of all resources.

If you want to authorize a Tencent Cloud service at the service level or authorize a service operation at the API level, you need to enter `*` for `resource` to grant the permission of all resources in the Tencent Cloud service or the `action` permission of all resources.

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:

©2013-2022 Tencent Cloud. All rights reserved.

```
qcs:project_id:service_type:region:account:resource
```

A six-segment resource description contains six fields as detailed below:

Field	Description and Valid Values	Required	Example
qcs	Tencent Cloud service abbreviation, which indicates a resource of Tencent Cloud.	Yes	qcs
project_id	Project information, which is only compatible with legacy CAM logic. It cannot be entered in	No	Empty

	the current policy syntax and can be left empty.		
service_type	Product (service) abbreviation. For more information, see "Abbreviation in CAM" in CAM-Enabled Products. If this field is left empty, it indicates all products.	No	CVM: cvm CDN: cdn
region	Region information. For more information on region names, see "Region List" in Common Params. If this field is left empty, it indicates all regions.	No	North China (Beijing): ap-beijing South China (Guangzhou): ap-guangzhou
account	Root account information of the resource owner. Currently, either `uin` or `uid` can be used to describe the resource owner. `uin` is the root account ID in `uin/${uin}` format. `uid` is the root account's `APPID` in `uid/${appid}` format, and only COS and CAS resource owners can be described in this way. If this field is left empty, it indicates the root account of the CAM user creating the policy.	No	uin: uin/12345678 uid: uid/10001234
resource	Resource details of the product. Currently, you can describe a resource in the following two formats: `resource_type/${resourceid}` and `<resource_type>/<resource_path>` . `resource_type/${resourceid}` : `resourcetype` is the resource prefix, which describes the resource type. `${resourceid}` is the specific resource ID, which can be viewed in the corresponding product console. `*` indicates all resources of this type. `<resource_type>/<resource_path>` : `resourcetype` is the resource prefix, which describes the resource type. `<resource_path>` is the resource path. This format supports directory-level prefix match.	Yes	CVM: instance/ins-1 TencentDB for MySQL: instanceI 1 COS: `prefix//10001234/bucket` which indicates all files in `bucke` Various COS resource types are supported. For more information, Working with COS API Authorizat Policies.

Definition of CAM Resources

CAM resources include users, user groups, and policies. A CAM resource can be described as follows:

Root 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

©2013-2022 Tencent Cloud. All rights reserved.

```
*
```

Policy

```
qcs::cam::uin/12345678:policyid/*
```

Or

```
qcs::cam::uin/12345678:policyid/12423
```

Notes on Resources

A resource owner is always a root account. The sub-account that creates a resource will not automatically have access to the resource without authorization; instead, it must be authorized by the resource owner.

Services such as COS and CAS support cross-account authorization for resource access. Authorized accounts can pass permissions to their sub-accounts through permission propagation.

Relevant Documents

For more information on service-specific resource definitions, see the corresponding product documentation in CAM-Enabled Products.

©2013-2022 Tencent Cloud. All rights reserved.

Policy Variable

Last updated：2024-01-23 17:54:33

Overview

Suppose you want to grant every CAM user the permission to access resources they create; for example, you want a user who created a COS resource to have the access to the resource by default.

If the resource owner (root account) authorizes the resources to the resource creator one by one, the owner needs to write policies for each resource and authorize it to the creator, which leads to high authorization costs. In this case, you can use policy variables to meet your requirements. A policy variable is a placeholder that describes the creator’s sub-account UIN in the resource definition. During authentication, the policy variable will be replaced by the contextual information of the request.

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}/*"
        }
    ]
}
```

©2013-2022 Tencent Cloud. All rights reserved.

A policy variable carries the creator's sub-account UIN in every resource path. For example, if a sub-account (with its own UIN being `125000000` and its root account's UIN being `1000001`) has created a CMQ message queue named `queueName/uin/125000000` in Chengdu region, the resource will be described as follows:

```
qcs::cmqqueue:ap-chengdu:uin/1000001:queueName/uin/125000000
```

When the above sub-account accesses this resource, the placeholder of the corresponding policy information will be replaced by the visitor during the authentication process, that is,

©2013-2022 Tencent Cloud. All rights reserved.

```
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 location: A policy variable can be in the last segment in a 6-segment resource description.

Condition element location: A policy variable 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 6-segment resource description of COS is `qcs::cos:$region:uid/$appid:$bucketname-$appid/$ResourcesPath` , in which `$ResourcesPath` indicates the specific resource path. The above policy variable cannot be used in `$ResourcesPath` . A complete 6-segment resource description of 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	Description
${uin}	The current visitor's sub-account UIN, or the root account UIN (if the visitor is a root account).
${owner_uin}	UIN of the root account to which the current visitor belongs.
${app_id}	APPID of the root account to which the current visitor belongs.

Conditions

Overview of Effective Conditions

Last updated：2024-01-23 17:54:33

When configuring access management policies, you can specify the conditions under which the policy takes effect. These conditions are optional. After the conditions are configured, 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 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 have 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"
               }
           }
```

©2013-2022 Tencent Cloud. All rights reserved.

Matching Logic for Effective Conditions

The evaluation logic for effective conditions is as follows:

Evaluation Logic	Note
Condition Fulfillment	A single condition key can have one or more condition values. During condition checking, if the value of the condition key matches any of the specified values, the condition is fulfilled.
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 for the condition clause to be deemed fulfilled.
Condition Block Fulfillment	The condition block is considered fulfilled only if all condition clauses within it are fulfilled simultaneously.
Condition operators (except null_equal) suffixed with if_exist	indicates 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, indicating that the policy will take effect if any of the condition values in the context information meets the requirements.

Note

Authorization by tag only supports 'for_any_value'.

Effective Condition Example

©2013-2022 Tencent Cloud. All rights reserved.

```
"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, for example, `192.168.1.1` . The type of comparison to be performed is specified by the condition operator (ip_equal in this example).

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` network segments 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：2024-01-23 17:54:33

When creating a policy through the Cloud Access Management Console's Creating Custom Policy,, you can set the policy's effective conditions as needed.

Condition Keys

The naming format for Tencent Cloud's general condition keys is: `qcs:<condition-key>` . Currently, only five condition keys are supported. The content and descriptions of these keys are as follows:

General 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:resource_tag	String	Controls 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	Determines 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.

©2013-2022 Tencent Cloud. All rights reserved.

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	Condition Operators	Description
String Condition Operators	string_equal	String is equal to (case-sensitive)
	string_not_equal	String is not equal to (case-sensitive)
	string_equal_ignore_case	String is equal to (case insensitive)
	string_not_equal_ignore_case	String is not equal to (case insensitive)
Numeric Condition Operators	numeric_equal	Number is 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 is less than or equal to
	date_greater_than	Date and Time Greater Than
	date_greater_than_equal	Date and time is greater than or equal to
Boolean Condition Operators	bool_equal	Boolean Value Matching
Binary Condition Operators	binary_equal	Number is equal to
IP Address Condition Operators	ip_equal	IP address is equal to
	ip_not_equal	IP address is not equal to
Empty Condition Key	null_equal	Empty Condition Key Matching

©2013-2022 Tencent Cloud. All rights reserved.

Operators		

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. For list-type interfaces, please see Overview.

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：2024-01-23 17:54:33

Scenario	Description	Sample
The condition operator contains a condition value of a condition key.	The VPC is allowed 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 contains multiple condition values of a single condition key.	Users with two specified IP addresses are allowed to access.	Example
Scenarios with multiple condition operators.	Users with a specified IP are allowed to access on the specified date.	Example
A single condition operator contains multiple condition keys.	Multiple condition keys are attached to a single condition operator.	Example
Application of Boolean Condition Operators	Sub-users must bind the token before they can delete the API key.	Example

The condition operator contains 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 check whether the CAM user has access permissions for the VPC associated with the peering connection.

Sample Code 1

In the following example, the VPC is allowed to be bound to a specified peering connection. The VPC region must be `Shanghai` :

```
{
   "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 contains multiple condition values of a single condition key.

Description

A single condition operator that contains multiple condition values of a condition key is evaluated using the logic OR. 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 describes 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",
```

©2013-2022 Tencent Cloud. All rights reserved.

```
                   "111.21.33.72/24"
               ]
           }
       }
   }
 ]
}
```

Scenarios with Multiple Condition Operators

Description

If your policy involves multiple condition operators, they are evaluated using the logic 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 in order to match.

```
"condition": {
               "ip_equal": {
                   "qcs:ip": "192.168.1.1"
               },
               "date_less_than": {
                   "qcs:current_time": "2022-05-31 00:00:00"
               }
           }
```

©2013-2022 Tencent Cloud. All rights reserved.

A single condition operator contains multiple condition keys.

Description

If your policy involves multiple condition operators or attaches multiple condition keys to a single condition operator, the conditions are evaluated using a logic AND.

Sample Code

The following example describes that it can be matched only if both the resource tag and the request tag are "Department & Research and Development".

©2013-2022 Tencent Cloud. All rights reserved.

```
"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": [
               "*"
           ],
```

©2013-2022 Tencent Cloud. All rights reserved.

```
                "condition": {
                    "bool_equal": {
                        "qcs:BindToken": "true"
                    }
                }
            }
    ]
}
```

Policy Version Control

Last updated：2024-01-23 17:54:33

Overview

When a custom policy you configured is changed, the system will not overwrite it; instead, it will automatically create a new version. After saving the change, you can configure a default version out of different versions for rapid rollback to different policy versions.

Granting Permission to Set Default Policy Version

Root accounts and sub-accounts that have permissions to use the `cam:ListPolicies` , `cam:GetPolicy` , and `cam:UpdatePolicy` APIs can configure a default policy version.
Root accounts can use the following policy syntax to grant sub-accounts permission to configure a default policy version:

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "name/cam:ListPolicies",
                "name/cam:GetPolicy",
                "name/cam:UpdatePolicy"
            ],
            "resource": [
                    "*"
                ]
            }
        ]
    }
```

Setting the default version of custom policy

You can set one of the custom policy versions as the default version to make it the active version. After the configuration, all sub-accounts associated with this custom policy will receive the permissions set on the default version.

1. Log in to the CAM console, and go to Policies.
2. On the policy management page, click the name of the custom policy you want to configure to enter the policy details page.
3. On the policy details page, select **Policy Version**.
4. Locate the version you want to configure, check the box on the left, and click **Save as Default**.

Rolling back Changes by Using Different Versions

You can roll back your changes by setting the default version of the custom policy. For example, see the following scenario:

You create a custom policy that allows sub-accounts to have read access to CVM instance `ins-1` . When you create the policy, there is only one version of the custom policy (tagged as "v1"). This version is automatically set as the default version, and this policy can work normally.

You update this custom policy and add read permission to CVM instance `ins-2` . After the change is saved, the system will create a new policy version (tagged as "v2"). After v2 is set as the default version, sub-accounts feed back that they lack the original CVM management permission. In this case, you can roll back the current policy version to v1. You can set v1 as the default version and restore the sub-account's management permission for the original CVM instance.

You find and correct an error in policy v2, and the system will create another new version of the policy (tagged as "v3"). You can set v3 as the default version to provide the sub-accounts with read permission to both CVM instances `ins-1` and `ins-2` . You can delete the policy v2 which contains the error.

Version Limits

©2013-2022 Tencent Cloud. All rights reserved.

Each custom policy can have up to 5 versions. When the number of versions of a custom policy reaches 5, you must delete one or more current versions before you can edit and save a new version. You can delete existing policy versions in the pop-up dialog box in the following two ways:

Delete the oldest non-default policy version.

Select one or more policy versions to be deleted. You can click ▼ on the left to view the policy syntax of each version to make decisions more conveniently.

Note:

When a version is deleted, version IDs of the remaining versions will not change. Therefore, version IDs may be discontinuous. For example, if you delete the policy v2 and v4 and then add two new versions, the remaining version IDs may be v1, v3, v5, v6, and v7.

Scenarios where 'deny' in permission policy is ineffective

Last updated：2024-01-23 17:54:33

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 describes 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 for Querying 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:

Scenario 1: If a sub-user is granted permission (allow) to access CVM instances a, b, and c, but denied (deny) to 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 the access to resources tagged with T2, and resource a is tagged with both T1 and T2, then the denial of access to resource a will not be effective.

For instance, even when the following policy is authorized, resource a can still be viewed when viewing the resource list.

```
{
   "version": "2.0",
   "statement": [
       {
           "effect": "allow",
           "action": [
               "*"
           ],
           "resource": "*",
           "condition": {
               "for_any_value:string_equal": {
```

©2013-2022 Tencent Cloud. All rights reserved.

```
                    "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, the statement is effective only if the condition keys support precise matching, such as 'string_equal', 'ip_equal', 'ip_not_equal', etc. If other types of condition keys (for example, 'string_not_equal', etc.) are included, the statement 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
                   ]
               }
           }
       }
   ]
}
```

Denying Access to COS of 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.

Troubleshooting

Creating Policy Based on Fault Report

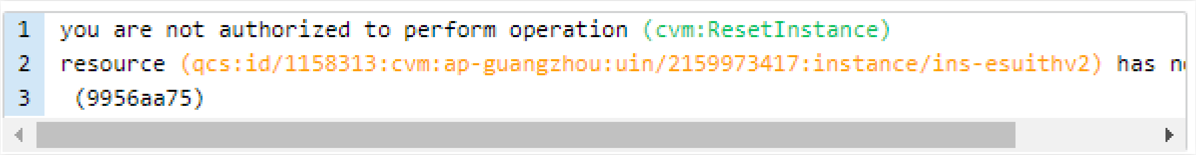
Last updated：2024-01-23 17:57:37

Overview

This document describes how to create a policy to resolve a fault according to the fault report. After the fault is resolved, the sub-account will be able to manage the resources of the root account within the scope of the newly configured permissions.

Example

When a sub-account associated with the `QcloudCVMReadOnlyAccess` policy attempts to reinstall a CVM instance, the following error is reported:



```
you are not authorized to perform operation (cvm:ResetInstance)
resource (qcs:id/1158313:cvm:ap-guangzhou:uin/2159973417:instance/ins-esuithv2) has n
 (9956aa75)
```

If you want to authorize the sub-account to proceed with this operation, you can create and associate a custom policy according to this error message.

Directions

1. Log in to the CAM console, enter the Policies page, and click **Create Custom Policy**.
2. In the selection window that pops up, click **Create by Policy Generator** to enter the **Edit Policy** page.
3. On the

Edit Po

licy page, set the following information:

Effect (required): select whether the operation is allowed. In this example, select "Allow".

Service (required): select the product based on the abbreviation to authorize. In this example, it is **CVM** corresponding to `cvm` in the `operation` field of the error message.

Action (required): select the operation to authorize. In this example, select **ResetInstance** corresponding to the `operation` field of the error message.

Resource (required): for products that don't support resource-level authorization, you can only select all resources as the authorization granularity. For products that support resource-level authorization, you can select a specific resource. To do so, click **Add a six-segment resource description** and enter the resource prefix and resource. In this example, the error message is for a specific resource, so you need to authorize it: select the specific resource, click **Add a six-segment resource description**, and then you can directly copy the prefix and resource in `qcs:id/1158313:cvm:ap-guangzhou:uin/2159973417:instance/instance/ins-esuithv2` and paste them.

Condition (optional): set the conditions that must be met for the permission to take effect, such as a specified access IP. In this example, leave it empty.

4. Click **Next** to enter the **Associate Users/User Groups** page.
5. On the **Associate Users/User Groups** page, add the policy name (automatically generated by the console) and description.

Note:

The policy name is `policygen` suffixed with the creation time by default, which is customizable.

The policy description corresponds to the service and operations selected in step 3. You can modify them as needed.

6. Click **Done** to complete the custom policy creation.
7. Authorize the sub-account as instructed in Authorization Management. After authorization, the sub-account will be granted the needed permission, and the fault will be resolved.

©2013-2022 Tencent Cloud. All rights reserved.

Creating Permissions Policy as Prompted

Last updated：2024-01-23 17:57:37

Overview

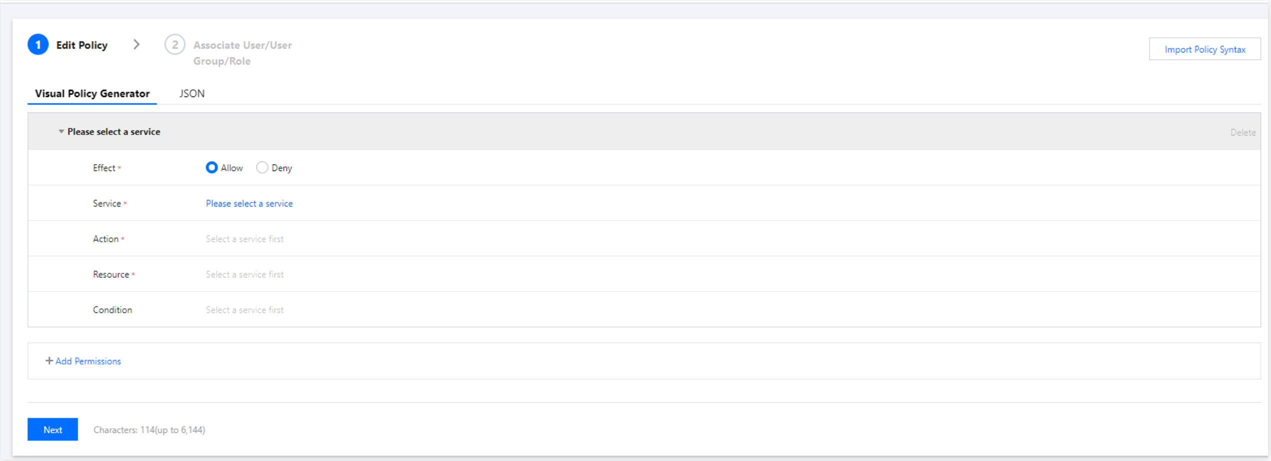
This document describes how to create a permissions policy when you are prompted for permission but do not have any. After the permissions policy is created, the sub-account can manage resources under the root account within the new permission scope.

Prerequisite

Your account is a root account or a sub-account with full read/write access (QcloudCamFullAccess).

Directions

1. Log in to the CAM console and go to Policies. Click **Create Custom Policy**.
2. In the pop-up window, click **Create by Policy Generator** to go to the **Edit Policy** page.
3. On the **Edit Policy** page, set the following information:



Effect * ● Allow ○ Deny

Service * Please select a service

Action * Select a service first

Resource * Select a service first

Condition Select a service first

Characters: 114(up to 6,144)

Effect (required): Select **Allow** or **Deny**. In this example, select **Allow**.
Service (required): Select the product by short name to authorize. In this example, it will be `cvm` referenced in the operation field in the error information.

Action (required): Select the action to authorize. In this example, select `RebootInstances` corresponding to the `operation` field in the error information.

Resource (required): For products that don't support resource-level authorization, you can only select all resources as the authorization granularity. For products that support resource-level authorization, you can select a specific resource. To do so, click **Add a 6-segment resource description** and enter the resource prefix and resource. In this example, the error message is for a specific resource, so you need to authorize it: Select the specific resource, click **Add a 6-segment resource description**, and then you can directly copy the prefix and resource in `qcs:id/0:cvm:ap-guangzhou:uin/10***6:instance/ins-arh4gyp2` and paste them.

Condition (required): Set the condition for the sub-account's authorization to take effect. `key` indicates the condition key, `ope` , the operator, and `value` , the condition value. In this example, `key` is `qcs:request_tag` , `ope` is `for_all_value:string_equal` , and `value` is `server&1024","a&b"` .

4. Click **Next** to go to the **Associate Users/User Groups** page.

5. On the **Associate Users/User Groups** page, add the policy name (automatically generated by the console) and description.

Note:

The policy name is `policygen` by default. The suffix number is generated based on the creation date. This is customizable.

The description corresponds to the service and action selected in Step 3. You can modify it as needed.

6. Click **Complete** to complete the custom policy creation.

7. Authorize the sub-account as instructed in Authorization Management. After successful authorization, the sub-account will be granted the required permission, and the error will be fixed.

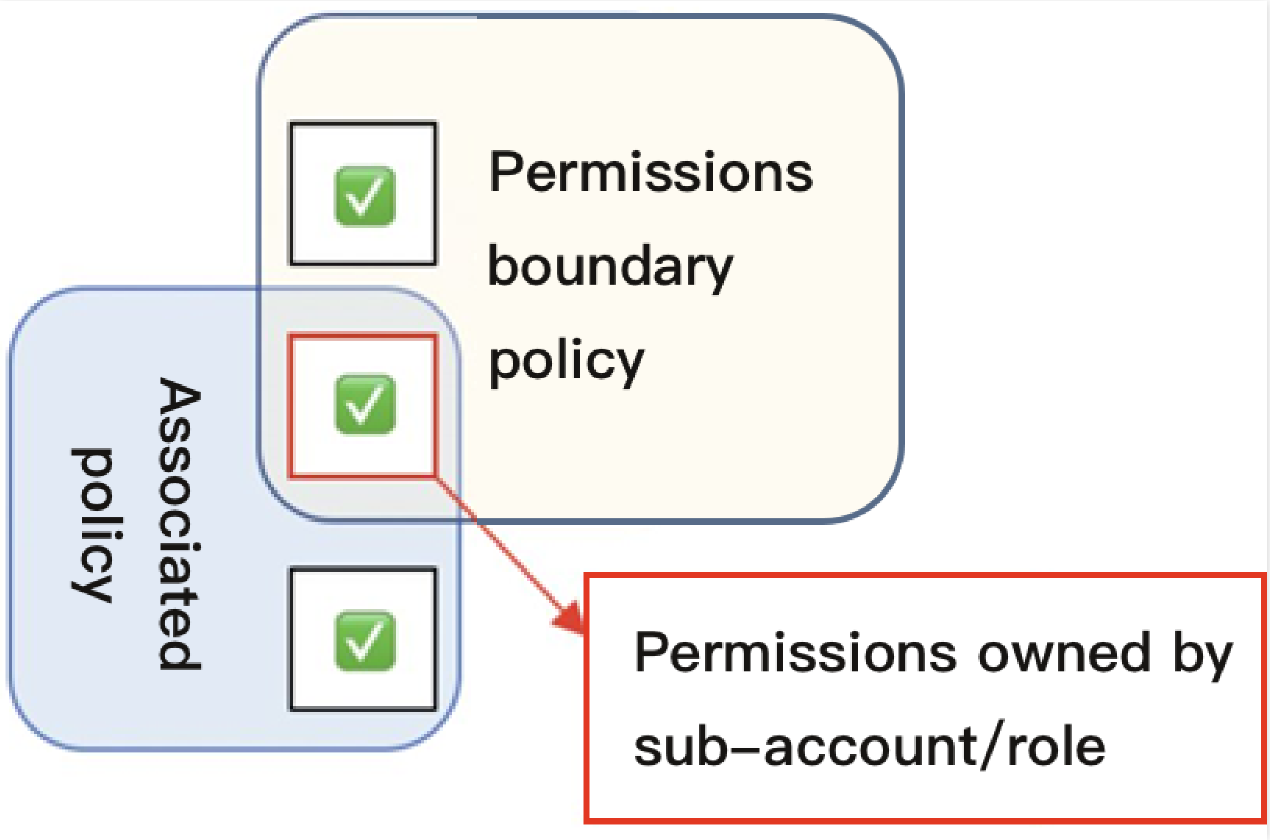
©2013-2022 Tencent Cloud. All rights reserved.

Permissions Boundary

Last updated：2024-01-23 17:57:37

Concept

Permissions boundary is an advanced feature used by Tencent Cloud to set a permissions boundary for a sub-account/role. After you set a permissions boundary for a sub-account/role, it can only perform operations allowed by both the associated policy and the permissions boundary. A permissions boundary only limits the maximum scope of permissions owned by a sub-account/role, but cannot be used to set permissions for the sub-account/role.


Permissions boundary policy
Associated policy
Permissions owned by sub-account/role

Overview

You can use a preset or custom policy to set permissions for a sub-account/role. This policy is the maximum scope of permissions that the sub-account/role can have. This document describes how to use a permissions boundary to set the maximum scope of permissions for a sub-account.

©2013-2022 Tencent Cloud. All rights reserved.

Suppose a company's Tencent Cloud resource admin needs to set permissions for Ops employees to meet the following requirements:

The company has two Ops employees, each with their own sub-account: 'test1' and 'test2'.

The employee with the sub-account `test1` only needs to manage all TencentDB for MySQL permissions under the root account.

The employee with the sub-account `test2` only needs to manage the operation permission for the server with the instance ID of `ins-1` under the root account.

The company stipulates that all operations on CVM and TencentDB for MySQL under the root account by sub-accounts must be performed in the IP range of the company (10.217.182.3/24 or 111.21.33.72/24).

Directions

Setting permissions for sub-account `test1`

1. Log in to the admin account and enter 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** section under the **Permission** tab, click **Associate Policy** and select the `QcloudCDBFullAccess` policy to set all TencentDB for MySQL permissions for the sub-account `test1` .
4. In the **Permissions Boundary** section under the **Permission** tab, click **Set Boundary** to enter the **Set Permissions Boundary** page.
5. On the permissions boundary setting page, click **Create Custom Policy** to enter the custom policy creation page.
6. On the custom policy creation 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 click **OK**.

Resource: The default value is **All resources (*)**.

Condition: Select **Source IP** and enter `10.217.182.3/24, 111.21.33.72/24` as the IP value.

8. Click **Create** to enter the permissions boundary setting page.
9. On the permissions boundary setting page, select the created custom policy in the policy list.
10. Click **Set Boundary**.

Setting permissions for sub-account `test2`

1. Log in to the admin account and create a custom policy syntax named `policygen-2` by referring to the following policy syntax. For more information, see Creating Custom Policy>>Creating by policy syntax.

```
{
 "version": "2.0",
 "statement": [
     {
         "effect": "allow",
         "resource":[
             "qcs::cvm:gz::instance/ins-1"
         ],
         "action": [
             "name/cvm:*"
         ]
```

```
        }
    ]
  }
```

2. On the user list page, find the sub-account `test2` and click the user's nickname to enter the user details page.

3. In the **Permissions Policy** section under the **Permission** tab, click **Associate Policy** and select the `policygen-2` policy to set the operation permission of the CVM instance named `ins-1` for the sub-account `test2` .

4. In the **Permissions Boundary** section under the **Permission** tab, click **Set Boundary** to enter the **Set Permissions Boundary** page.

5. On the permissions boundary setting page, click **Create Custom Policy** to enter the custom policy creation page.

6. On the custom policy creation page, set the policy name to **policygen-3**.

7. In **Visual Policy Generator**, add the following information:

Effect: Select **Allow**.

Service: Select **CVM**.

Action: Select **All actions** and click **OK**.

Resource: The default value is **All resources (*)**.

Condition: Select **Source IP** and enter `10.217.182.3/24, 111.21.33.72/24` as the IP value.

8. Click **Create** to enter the permissions boundary setting page.

9. On the permissions boundary setting page, select `policygen-3` in the policy list.

10. Click **Set Boundary** to complete the permission setting process.

©2013-2022 Tencent Cloud. All rights reserved.

Downloading Security Analysis Report

Last updated：2024-01-23 17:57:37

Overview

You can download a user credential report to view the credential status of all Tencent Cloud sub-accounts and their sub-users, as well as the console login password, access key and account security settings. This report can also be used for compliance audit.

Directions

1. Log in to the CAM console, and click **Overview** in the left sidebar.
2. In the “Security Analysis Report” module, click **Download User Credential Report** and complete identity verification as prompted. Then the report will be automatically generated.
3. After downloading the report, you can 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 format. You can use common spreadsheet software to open the CSV file for further analysis or use the file programmatically and perform custom analysis.

The CSV file contains the following information:

Field	Description	Value
AccountID	Account ID	Sub-account ID
Username	Username	Sub-account username
UserType	User type	`Sub-user` : sub-user `Collaborator` : collaborator `WeWork-Sub-user` : WeCom sub-user `Message-receiver` : message recipient
CreationTime	Creation time	Sample value: 2019/8/16 9:25:56

©2013-2022 Tencent Cloud. All rights reserved.

PasswordEnabled	Whether the console login password is enabled	`TRUE` : enabled `FALSE` : disabled. Console access is disabled and the login password is not set. `not_supported` : not supported. A WeCom sub-user logs in by scanning the QR code without a password. A message recipient only receives messages and does not have a password. A collaborator logs in as a root account and is not subject to this field.
PasswordLastRotation	Time when the password was last modified	`FALSE` : Console access is disabled and the login password is not set. `not_supported` : not supported. A WeCom sub-user logs in by scanning the QR code without a password. A message recipient only receives messages and does not have a password. A collaborator logs in as a root account and is not subject to this field.
LoginConsoleActive	Whether console login is supported	`TRUE` : enabled `FALSE` : disabled `not_supported` : not supported. A message recipient only receives messages and does not have a login password. A collaborator logs in as a root account and is not subject to this field.
LoginProtectionActive	Whether login protection is enabled	`TRUE` : enabled `FALSE` : disabled `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
OperationProtectionActive	Whether operation protection is enabled	`TRUE` : enabled `FALSE` : disabled `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
MFADeviceActive	Whether MFA is enabled	`TRUE` : enabled `FALSE` : disabled `not_supported` : not supported. A message recipient only receives messages and does not have a login password. The sub-user

		has not been bound to a mobile number or WeChat account.
Abnormal LoginsNumWithin30Days	Whether suspicious login behavior is detected in 30 days	`TRUE` : suspicious login behavior detected `FALSE` : suspicious login behavior not detected
AccessKey1SecretId	SecretId of key 1	`N/A` : no key
AccessKey1MayBeAtRisk	Whether key 1 has leakage risk	`TRUE` : at risk `FALSE` : no risk `N/A` : no key 1 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey1CreationTime	Creation time of key 1	`N/A` : no key 1 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey1Status	Status of key 1	`Active` : enabled `Disable` : disabled `N/A` : no key 1 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey1lastUsedDate	Time when key 1 was last used	`N/A` : no key 1 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey1CreatedOver90Days	Whether key 1 has been created for over 90 days	`N/A` : no key 1 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey1CreatedOver30Days	Whether key 1 has been created for over 30 days	`N/A` : no key 1 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey2SecretId	SecretId of key 2	`N/A` : no key 2
AccessKey2MayBeAtRisk	Whether key 2 has	`TRUE` : at risk

©2013-2022 Tencent Cloud. All rights reserved.

	leakage risk	`FALSE` : no risk `N/A` : no key 2 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey2CreationTime	Creation time of key 2	`N/A` : no key 2 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey2Status	Status of key 2	`Active` : enabled `Disable` : disabled `N/A` : no key 2 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey2lastUsedDate	Time when key 2 was last used	`N/A` : no key 2 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey2CreatedOver90Days	Whether key 2 has been created for over 90 days	`N/A` : no key 2 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.
AccessKey2CreatedOver30Days	Whether key 2 has been created for over 30 days	`N/A` : no key 2 `not_supported` : not supported. A message recipient only receives messages and does not have a login password.

©2013-2022 Tencent Cloud. All rights reserved.