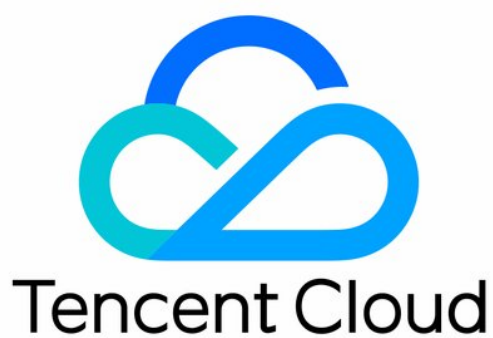


Chat

Console Guide

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

Trademark Notice



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

Service Statement

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

Contents

Console Guide

- Creating and Upgrading an Application

- Basic Configuration

- Feature Configuration

- Account Management

- Group Management

- Webhook Configuration

- Statistics

- Auxiliary Development Tools

- Access Management

 - Granting Console Operation Permissions to Sub-accounts

 - Preset Policy

 - Custom Policy

Console Guide

Creating and Upgrading an Application

Last updated : 2024-02-07 17:33:32

Use Cases

This document describes how to create Developer edition apps and obtain SDKAppIDs. It also covers how to upgrade Developer edition apps to Standard or Premium edition in the Chat console.

Prerequisite

You have signed up for a [Tencent Cloud account](#) and set a payment method.

Creating a Developer Edition App

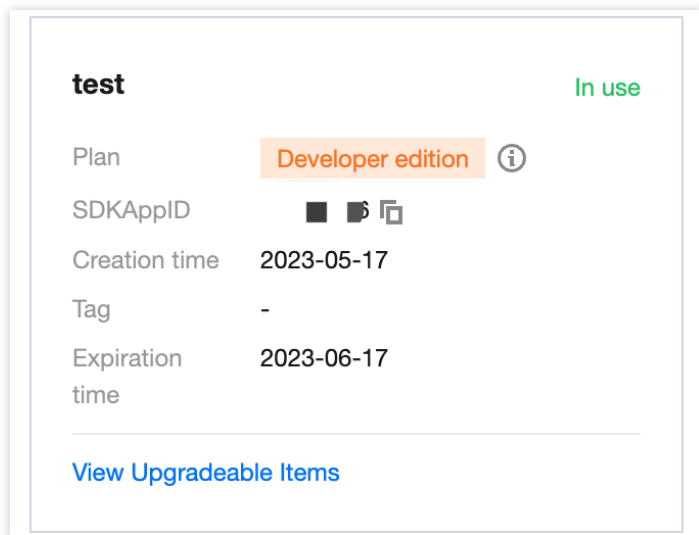
1. Log in to the [Chat console](#).
2. Click **Create Application**.
3. In the **Create Application** dialog box, enter your app name, and click **Confirm**.

After the app is created, you can view the status, service version, SDKAppID, creation time, and expiration time of the new app on the overview page of the console.

Note

By default, a new app is of Developer edition and enabled.

A Tencent Cloud account can create a maximum of 300 Chat apps. If you want to create a new app, [disable and delete](#) an unwanted app first. **Once an app (along with its SDKAppID) is deleted, the service it provides and all its data are lost. Proceed with caution.**



Upgrading an App

Note

You can upgrade your app to Standard or Premium edition but cannot roll it back to Developer edition after the upgrade. After an app is suspended due to overdue payment or refunds, you can [renew](#) a Standard or Premium edition plan to resume its services. If you want to go back to the Developer edition, [create a new app](#).

1. Click **View Upgradeable Items** in the target app section to view the upgradeable configuration items.

Compare Upgradeable Items

Item	Current Spec	After Upgrade to Standard - Prepaid	After Upgrade to Premium - Prepaid
Max Users	100	Unlimited ↑	Unlimited ↑
Max Friends	20	3000 ↑	3000 ↑
Max Groups One Can Join	50	500 ↑	1000 ↑
Max Audio-Video Groups	10	50 ↑	Unlimited ↑
Max Members per Non-Audio-Video Group	20	200 ↑	2000 ↑
Free Peak Groups	100 groups/month	Unlimited ↑	Unlimited ↑
Free peak MAU limit	100 MAU/month	10000 MAU/month ↑	10000 MAU/month ↑
Historical Message Storage	7 days	7 days	30 days ↑
Audio/video call	Not activated	Can increase to Group call version ↑	Can increase to Group call version ↑
Concurrent logins on multiple devices on the same platform	Supported	Unsupported	Supported
User status, pushing to all users and other features	Supported	Unsupported	Supported
Read receipts for group messages, targeted group messages and other features	Supported	Unsupported	Supported
Message history for new members, list of online members, broadcast messaging and other features of the audio-video group	Supported	Unsupported	Supported
Community, topic and other features	Supported	Unsupported	Supported

Upgrade Plan

2. Click **Upgrade Plan**, select configurations to be upgraded, select I have read and agree to the Billing Details, and then click **Upgrade Now**.

Basic Configuration

Last updated : 2024-02-07 17:33:32

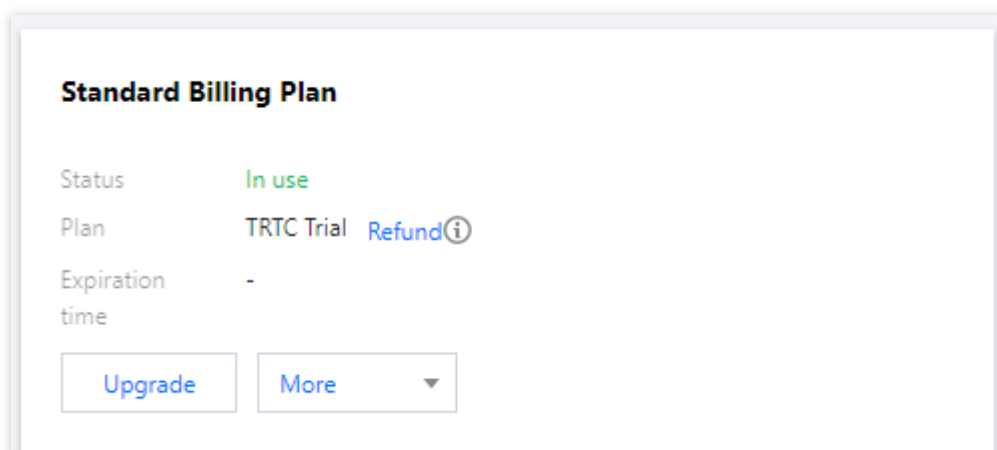
Log in to the [IM console](#) and click the target app card to go to the basic configuration page of the app. On the page, you can manage the basic configuration of the app based on your business needs.

Standard Billing Plan Information

In the **Standard Billing Plan** section, you can see the standard billing plan information of the app and perform the following operations:

Upgrade the standard billing plan of the app.

Disable/Delete the app.



Upgrading the standard billing plan

You can click **Upgrade Plan** in the **Standard Billing Plan** section to update the plan edition or configuration of your app. For more information, see [Upgrading an App](#).

Extending the Developer Edition Validity Period

If the plan for your app is Developer and its one-month validity period has expired, the app will be suspended. To continue using the **Developer edition** for testing and development, go to the Chat console to **apply for an extension** of the Developer edition validity period.

1. Log in to the [Chat Console](#) and click the target app card to go to the **Basic Configuration** page of the app.
2. Click **Apply for extension** in the **Standard Billing Plan** section.
3. Click **OK** to complete the application for extending the Developer edition validity period for one month.

Disabling/Deleting an app

Notes:

You can create up to 300 IM apps under a Tencent Cloud account. If you have reached that limit, [disable and delete] an unwanted app before creating a new one.

Only apps in "Disabled" status can be deleted. Once an app is deleted, all the data and services associated with the SDKAppID are removed and cannot be recovered, so proceed with caution.

Developer edition Apps

Developer edition apps can be manually disabled.

In the **Basic Info** area, click **Disable** next to **Status**. In the pop-up dialog box, click **OK**.

Developer edition apps can be manually deleted.

In the **Basic Info** area, click **Delete** next to **Status**. In the pop-up dialog box, click **OK**.

Pro and Premium edition Apps

Apps that have overdue payments for seven days will be automatically **Disabled**. To delete such disabled apps, [contact us](#).

Apps become **Expired** after refund, and **Disabled** after seven days. To delete such disabled apps, [contact us](#).

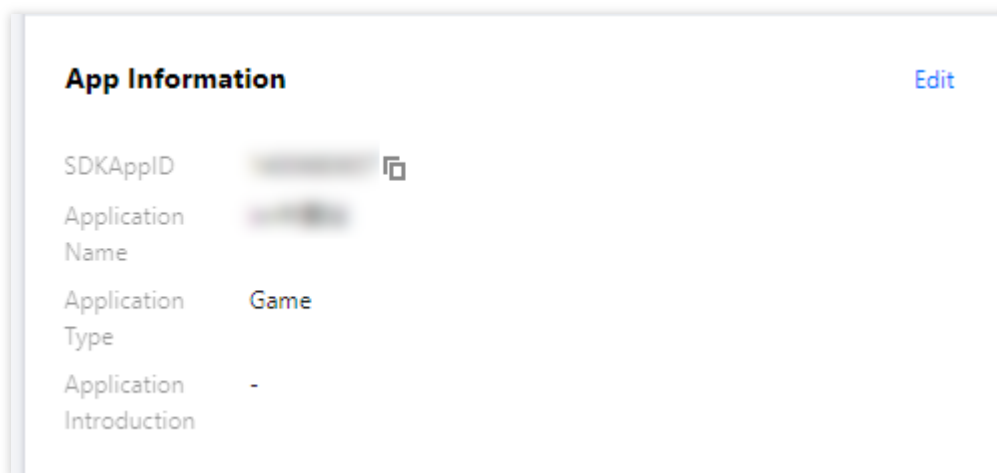
TRTC Developer edition Apps

Once a TRTC trial app is disabled by the TRTC administrator, you can [contact us](#) to disable and delete the app.

Configuring App Information

In the **Basic Info** section, you can:

Edit the basic information of your app, including the app name, type, and introduction.



The screenshot shows the 'App Information' configuration page. At the top left is the title 'App Information' and at the top right is a blue 'Edit' button. Below the title, there are five rows of configuration items, each with a label on the left and a value on the right. The first row is 'SDKAppID' with a blurred value and a copy icon. The second row is 'Application Name' with a blurred value. The third row is 'Application Type' with the value 'Game'. The fourth row is 'Application Introduction' with the value '-'. The fifth row is partially visible and appears to be another configuration item.

App Information		Edit
SDKAppID	[blurred]	[copy icon]
Application Name	[blurred]	
Application Type	Game	
Application Introduction	-	

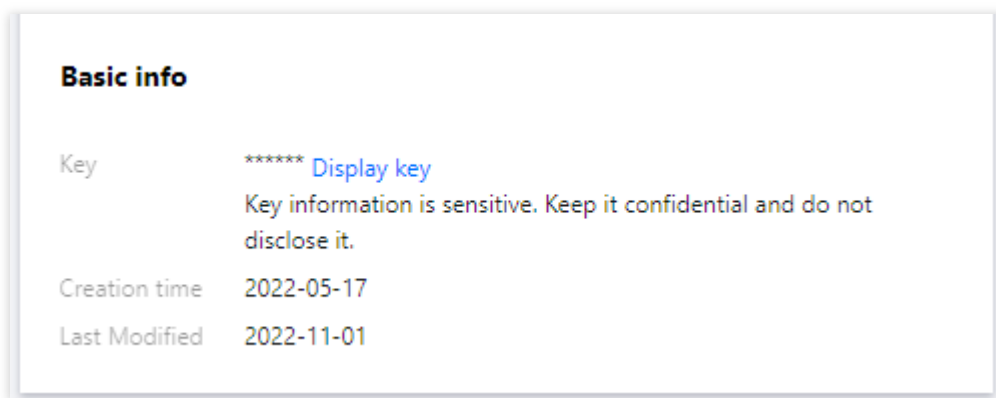
Editing basic information

1. Click **Edit** on the right of **Basic Info** to edit the app settings.
2. You can modify the app name, type, and introduction.
3. Click **Save**.

Configuring Basic Information

In the **Basic Information** section, you can:

Obtain the key of the app.



Obtaining a key

Keys are sensitive information. Be sure to keep them confidential and prevent them from being leaked. By default, apps (SDKAppIDs) created before August 15, 2019 use the [ECDSA-SHA256](#) signature algorithm that uses a public key and a private key. You can choose to update to the HMAC-SHA256 signature algorithm.

1. Click **Display key** to the right of **Key**.
2. Click **Copy** to copy and save the key information.

The key can be used to generate UserSig. For more information, see [Generating UserSig](#).

Managing Offline Push Certificates

Adding an offline push certificate

1. Click **Add Certificate** in the push settings area of the corresponding platform.
2. In the **Add Certificate** dialog that pops up, set the parameters as needed.

Adding an Android certificate

Add Android Certificate

Push Platform

☐ Mi ☐ Huawei ☒ Google ☐ Meizu ☐ Vivo ☐ OPPO ☐ Honor

Adding Method

☒ Upload certificate ☐ Enter the server key

Upload certificate

Select file

[How to Generate an FCM certificate](#)

ChannelID

Enter a channel ID

Confirm

Adding an iOS certificate

Add iOS Certificate

Push Type

☒ APNs Push ☐ VoIP Push

Certificate Type

☒ Production environment ☐ Development Environment

iOS certificate
(.p12) *

Select file

[How to generate an APNs certificate?](#)

Certificate
password *

Enter the certificate password

Confirm

3. Click **Confirm** to save the configuration.

Editing an offline push certificate

1. Click **Edit** in the certificate area.
2. In the dialog box that pops up, modify the parameters as needed and click **Confirm** to save the configuration.

Deleting an offline push certificate

Caution:

Once the certificate is deleted, push messages are no longer delivered. Deleted certificates cannot be restored. Proceed with caution.

1. Click **Delete** in the certificate area.
2. In the pop-up dialog box, click **Confirm**.

Configuring Tags

Editing tags

1. Click **Edit** on the right of **Tag Configuration**.
2. In the pop-up dialog, you can add or delete a tag.

Edit Tags ×

The tag is used to manage resources by category from different dimensions. If the existing tag does not meet your requirements, please go to [Manage Tags](#) ↗

1 resource selected

Tag key ▼

Tag value ▼

×

[+ Add](#)

OK

Cancel

TRTC

To implement features such as audio/video call and interactive live streaming in the current IM application, click **Activate** in the top-right corner of the **TRTC** section to quickly activate **TRTC**. The system will create a TRTC application in the **TRTC console**, which has the same `SDKAppID` as your current IM application. The two can use the same accounts and authentications.

After activation, you can click **View application** in the top-right corner of the **TRTC** section to view your TRTC application in the TRTC console.

Call

Call is one of the Value-Added Services of Chat. It is a call component jointly provided by TRTC and Chat.

1. Activate the free edition of Call

Click on **try now**.

After confirming the content of the pop-up window, click **activate now** to activate the free edition of Call. Once finished, you can proceed with integration according to [integration guide](#).

Each application (`SDKAppID`) can apply TRTC Call twice, and the total number of trial opportunities for all `SDKAppID` under one account (UIN) is 10. The number of trials redeemed during the beta testing period will also be counted in this total. If the free edition (`SDKAppID`) has not yet expired, you can easily apply for the second trial opportunity by clicking on **edition details - renew trial**, and the validity period of the free edition will be extended for 7 days.

2. Purchase the official editions of Call

Click **buy now**.

Make your selections in the pop-up purchase window, and click **Buy Now** after confirmation.

3. View the details of Call

If you have activated Call, you can click **edition details** to view the details of the Call.

If you want to check the usage of the Call, please visit the [TRTC console](#).

Feature Configuration

Last updated : 2024-03-06 14:54:21

Login and Message

Log in to the [IM console](#), click the target app section, and select **Feature Configuration > Login and Message** on the left sidebar. You can manage login and message related settings according to your business needs.

Login settings

1. On the **Login and Message** page, click **Edit** in the upper-right corner of the **Login Settings** area.
2. In the pop-up dialog box, select a multi-device login policy and set the maximum number of concurrent online web instances.

Note

If you select multi-device login for the Premium edition, up to 10 concurrent online web clients are supported, and up to 3 online devices are supported for each of the Android, iPhone, iPad, Windows, macOS, and Linux platforms.

Login settings

Multi-device Login Type

☐ **Single-device login** allows single-device login across web, Windows, Android, devices.

☒ **Dual-device login** allows single-device login across Windows, Android, or iOS, simultaneous online on a web browser.

☐ **Triple-device login** allows single-device login across Android and iOS, plus simultaneous online on both Windows devices and web browser.

☐ **Multi-device online** allows users to stay online simultaneously on web, Windc and iOS devices.

Online Web Instances

1

Confirm

Cancel

3. Click **Confirm**.

Historical message storage period settings

Historical messages are stored for seven days by default. **Extending the storage period is a value-added service.** For more information on billing, see [Pricing](#). You can modify the storage period once every month.

1. On the **Login and Message** page, click **Edit** in the upper-right corner of the **Historical Message Storage Period Settings** area.
2. In the pop-up dialog box, extend the storage period of historical messages.
3. Click **Confirm** and the configuration will take effect immediately.

Message recall settings

1. On the **Login and Message** page, click **Edit** in the upper-right corner of the **Message Recall Settings** area.
2. In the pop-up dialog box, set the time limit for message recall.
3. Click **Confirm**.

Multi-client synchronization settings

You can enable or disable **Sync Conversation Deletion Across Clients** in the **Multi-client Synchronization Settings** area on the **Login and Message** page.

Enabled: If multiple clients are online concurrently, deleting a conversation from one client will be synced to other clients (that is, the conversation will also be deleted from other clients).

Disabled: If multiple clients are online concurrently, deleting a conversation from one client will not be synced to other clients. The feature of syncing conversation deletion across clients is disabled by default.

Note

The feature of syncing conversation deletion across clients is available only to **native SDK v5.1.1 and web SDK v2.14.0 or later**. If you are using an earlier SDK version, you need to **upgrade your SDK** before you can use the feature.

User status query and status change notification settings

You can enable the feature of user status query and status change notification in the **Set user status query and status change notification** area on the **Login and Message** page.

Note

The feature of user status query and status change notification is disabled by default. When it is disabled, the error code 72001 will be reported for user status query, subscription, or unsubscription on clients. The feature can be enabled on native SDK v6.3 or later and is available only to Premium edition users. You can [click here to upgrade](#).

Message extension settings

You can enable message extension in the **Set message extension** area on the **Login and Message** page.

Note

Message extension allows you to configure keys and values for messages to implement features such as polling, group notices, and surveys. For more information, see [here](#). Message extension is available only to Premium edition

users and is supported only on native SDK Enhanced edition v6.7.3184 or later. If you are using an earlier version, upgrade your SDK.

"Pushing to all users" settings

You can enable the feature of pushing to all users in the **Push to all users** area.

Note

Pushing to all users is an excellent tool for application user operations. It not only supports sending specific content to all users, but also can send personalized content to specific user groups based on tags and attributes, such as member events, and regional notifications. This helps effectively attract, convert, and activate users. For more information, see [Pushing to All Users](#).

Configuration of conversations to pull

In the **Configuration of conversations to pull** area on the **Login and Message** page, you can configure the number of conversations to be pulled from the cloud. The default number is 100, and you can change the number to up to 500.

Note

The feature of configuring the number of conversations to pull is available only to **Premium edition** users. If you are not an Premium edition user, you need to upgrade your package before you can use the feature.

The feature of configuring the number of conversations to pull is available only to **native SDK v5.1.1 and web SDK v2.0 or later**. If you are using an earlier SDK version, you need to upgrade your SDK before you can use the feature.

Blocklist check

You can enable or disable **Show "Sent successfully" After Sending Messages** in the **Blocklist check** area on the **Login and Message** page.

Enabled: If you are in the recipient's blocklist, you will see **Sent successfully** after sending a one-to-one message and the recipient will not receive the message. This is the default setting.

Disabled: If you are in the recipient's blocklist, you will see **Failed to send** after sending a one-to-one message.

Relationship check

You can enable or disable **Check Relationship for One-to-One Messages** in the **Relationship Check** area on the **Login and Message** page.

Enabled: Check relationships before a one-to-one chat starts and only allow sending one-to-one messages to friends. When a user sends a one-to-one message to a stranger, the SDK will return [error code 20009](#).

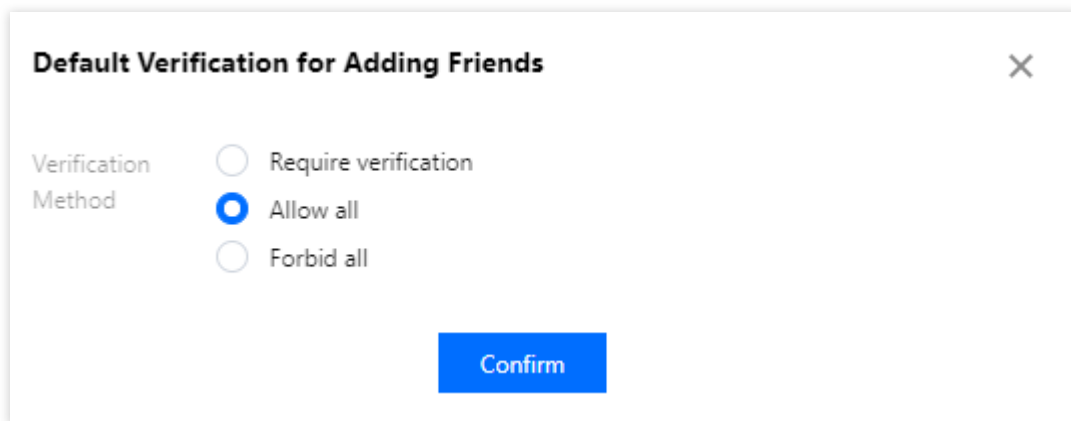
Disabled: Do not check relationships before a one-to-one chat starts and allow users to send and receive one-to-one messages to and from friends and strangers. This is the default setting.

Friends and Relationship Chain

Setting verification method for adding friends and custom friend fields.

Verification method for adding friends

1. Log in to the [IM console](#) and click the target IM app section.
2. On the left sidebar, choose **Feature Configuration > Friend and Relationship**, and click **Edit** in the upper-right corner of the **Default Verification for Adding Friends** area.



Default Verification for Adding Friends ✕

Verification Method

☐ Require verification

☒ Allow all

☐ Forbid all

Confirm

3. Select a verification method as needed and click **Confirm**.

Custom friend fields

Note

You can add up to 20 custom friend fields, which cannot be deleted and whose field name and type cannot be modified. Please set the fields properly as needed.

1. Log in to the [IM console](#) and click the target IM app section.
2. On the left sidebar, choose **Feature Configuration > Friend and Relationship**.
3. Click **Add** in the upper-right corner of the **Custom Friend Field** area.
4. In the pop-up dialog box, enter a field name and select a field type.

Note

The field name must be all letters and cannot exceed eight characters.

Custom User Fields

Log in to the [IM console](#), click the target app section, and select **Feature Configuration > Custom User Field** on the left sidebar. You can manage custom user fields according to your business needs.

Caution

You can add up to 20 custom user fields, which cannot be deleted and whose field name and type cannot be modified. Please set the fields properly as needed.

Adding a custom user field

1. On the **Custom User Field** page, click **Add** in the upper-right corner.
2. In the pop-up dialog box, enter a field name, select a field type, and set read/write permissions.

Note

The field name must be all letters and cannot exceed eight characters.
You need to enable at least one read permission and one write permission

User Custom Fields [Close]

Custom Field*

Field Type

Readable by App ☐ Activate ☒ Disable

Writable by App ☐ Activate ☒ Disable

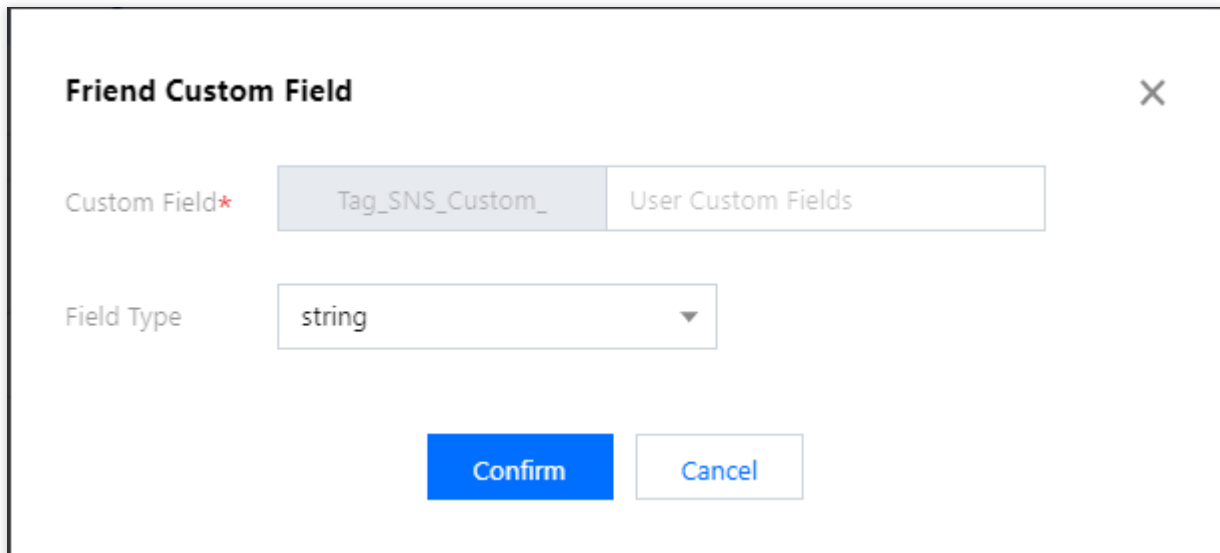
Readable by Administrator ☐ Activate ☒ Disable

Writable by Administrator ☐ Activate ☒ Disable

3. Click **Confirm**.

Modifying the permissions of a custom user field

1. On the **Custom User Field** page, click **Change Permissions** in the row of the target field.
2. In the pop-up dialog box, change the read or write permission.
3. Click **Confirm**.



Friend Custom Field [X]

Custom Field*

Field Type

4. Click **Confirm**.

Group Configuration

Custom group member fields

Log in to the [IM console](#), click the target app section, and select **Feature Configuration > Custom Group Member Field** on the left sidebar. You can manage custom group member fields according to your business needs.

Caution

You can add up to five custom group member fields, which cannot be deleted and whose group type and read/write permissions can be changed. Please set the fields properly as needed.

Adding a custom group member field

1. On the **Custom Group Member Field** page, click **Add** in the upper-right corner.
2. In the pop-up dialog box, enter a field name and set group types and read/write permissions.

Note

The field name can contain up to 16 characters, supporting letters, digits, and underscores (_). It cannot begin with a digit.

A custom group member field and a custom group field cannot have the same name.

Click **Add Group Type** to add one group type at a time. Duplicate group types are not allowed.

Click **Delete** in the row of the target group type to delete it. However, you must retain at least one group type.

Group Member Custom Field

Field Name

A field name can contain up to 16 characters and only letters, numbers, and underscores are supported. It can

Group Type

Group Type	Read	Write	My Own Readable Writable
<div>Work Group</div>	<div>Readable by All</div>	<div>Writable by All</div>	<div>Readable and Wri</div>

Add Group Type

☒ I understand that after a "group member custom field" is added, only the read-write permissions of the ac
the group type cannot be reselected or deleted; the field cannot be deleted.

Confirm

Cancel

3. Select **I understand that after a custom group member field is added, only the read-write permissions of the added group type can be modified; the group type cannot be reselected or deleted; the field cannot be deleted.**

4. Click **Confirm**.

Editing a custom group member field

1. On the **Custom Group Member Field** page, click **Edit** in the row of the target custom group member field.
2. In the pop-up dialog box, modify the read and write permissions of existing group types, or click **Add Group Type** to add a new one and set its parameters. Duplicate group types are not allowed.

Group Member Custom Field

Field Name

test

A field name can contain up to 16 characters and only letters, numbers, and underscores are supported. It can

Group Type

Group Type	Read	Write	My Own Readable Writable
Work Group	Readable by All	Writable by All	Readable and Writ
Public Group	Readable by All	Writable by All	Readable and Writ
Meeting Group	Readable by All	Writable by All	Readable and Writ

Add Group Type

☒ I understand that after a "group member custom field" is added, only the read-write permissions of the ad the group type cannot be reselected or deleted; the field cannot be deleted.

Confirm

Cancel

3. Select **I understand that after a custom group member field is added, only the read-write permissions of the added group type can be modified; the group type cannot be reselected or deleted; the field cannot be deleted.**

4. Click **Confirm**.

Custom group fields

Log in to the [IM console](#), click the target app card, and select **Feature Configuration > Custom Group Field** on the left sidebar. You can manage custom group fields according to your business needs.

Caution

You can add up to 10 custom group fields. Once set, these fields cannot be deleted, and only the group types and the corresponding read and write permissions can be modified. Therefore, set these fields properly as needed.

Adding a custom group field

1. On the **Custom Group Field** page, click **Add** in the upper-right corner.

2. In the pop-up dialog box, enter a field name and set the group types and read/write permissions.

Note

The field name can contain up to 16 characters, supporting letters, digits, and underscores (_). It cannot begin with a digit.

A custom group field and a custom group member field cannot have the same name.

Click **Add Group Type** to add one group type at a time. Duplicate group types are not allowed.

Click **Delete** in the row of the target group type to delete it. However, you must retain at least one group type.

Group-level Custom Field

Field Name

A field name can contain up to 16 characters and only letters, numbers, and underscores are supported. It can

Group Type

Group Type	Read	Write
<div>Public Group</div>	<div>Readable by All</div>	<div>Writable by All</div>

Add Group Type

☒ I understand that after a "group custom field" is added, only the read-write permissions of the added group type cannot be reselected or deleted; the field cannot be deleted.

Confirm

Cancel

3. Select **I understand that after a custom group member field is added, only the read-write permissions of the added group type can be modified; the group type cannot be reselected or deleted; the field cannot be deleted.**

4. Click **Confirm**.

Editing a custom group field

1. On the **Custom Group Field** page, click **Edit** in the row of the target custom group field.

2. In the pop-up dialog box, modify the read/write permissions of existing group types, or click **Add Group Type** to add a new one and set its parameters. Duplicate group types are not allowed.

Group-level Custom Field

Field Name

test1

A field name can contain up to 16 characters and only letters, numbers, and underscores are supported. It can

Group Type

Group Type	Read	Write
<div>Public Group</div>	<div>Readable by Member</div>	<div>Writable by All</div>
<div>Work Group</div>	<div>Readable by All</div>	<div>Writable by All</div>
<div>Meeting Group</div>	<div>Readable by All</div>	<div>Writable by All</div>

Add Group Type

☐ I understand that after a "group custom field" is added, only the read-write permissions of the added group type cannot be reselected or deleted; the field cannot be deleted.

Confirm

Cancel

3. Select **I understand that after a custom group member field is added, only the read-write permissions of the added group type can be modified; the group type cannot be reselected or deleted; the field cannot be deleted.**

4. Click **Confirm**.

Group message configuration

Log in to the [IM console](#), click the target application section, select **Feature Configuration > Group configuration > Group message configuration** on the left sidebar, and configure group messages as needed.

Pulling message history before group join

1. On the **Pull message history before group join** page, select a **Group Type** and click **Edit**.
2. In the **Pull message history before group join** pop-up window, select the required configuration items.

Note

It takes about ten minutes for the configuration to take effect.

Audio-video groups do not support this configuration.

Group system notification configuration

Log in to the [IM console](#), click the target application section, select **Feature Configuration > Group configuration > Group system notification configuration** on the left sidebar, and configure group system notifications as needed.

Notification of group member change

1. On the **Notification of group member change**, select a **Group Type** and click **Edit**.
2. In the **Notification of group member change** pop-up window, select the required configuration items.

Note

It takes about ten minutes for the configuration to take effect.

Audio-video groups do not support configuring the notification of group member change.

Notification of group profile change

1. On the **Notification of group profile change** page, select a **Group Type** and click **Edit**.
2. In the **Notification of group profile change** pop-up window, select the required configuration items.

Note

It takes about ten minutes for the configuration to take effect.

Audio-video groups do not support configuring the notification of group profile change.

Notification of group member profile change

1. On the **Notification of group member profile change** page, select a **Group Type** and click **Edit**.
2. In the **Notification of group member profile change** pop-up window, select the required configuration items.

Note

It takes about ten minutes for the configuration to take effect.

Group feature configuration

Log in to the [IM console](#), click the target application section, select **Feature Configuration > Group configuration > Group feature configuration** on the left sidebar, and configure the group feature as needed.

Community

A community is a large group that can hold up to 100,000 users. Once a community is created, it allows users to join or leave freely and supports historical message storage. The community feature is disabled by default. Enabling it allows you to create communities and use associated features.

If you need to use the topic feature, enable it after creating a community. Multiple topics can be created under the same community, and they share the same set of community member relationships. However, different topics have their own message sending and receiving independently and do not interfere with each other.

Note

The community feature is available only for native SDK v5.8.1668 enhanced edition or later and for web SDK v2.17.0 or later. If you are using an earlier SDK version, you need to upgrade your SDK before you can use the feature.

This feature is available only for Premium edition users. You can [click here to upgrade](#).

List of online audio-video group members

The feature of "List of online audio-video group members" is disabled by default. You can enable it as needed.

Note

If the feature is enabled, the list of the 1,000 latest online members of an audio-video group will be stored and the list can be pulled on clients.

This feature is available only for native SDK v6.3 or later. If you are using an earlier SDK version, you need to upgrade your SDK before you can use the feature.

This feature is available only for Premium edition users. You can [click here to upgrade](#).

Broadcast messaging of audio-video group

Broadcast messaging of audio-video group is disabled by default. You can enable it as needed.

Note

Broadcast messaging of audio-video group is disabled by default and can be enabled on native SDK v6.5 or later. Enabling this feature allows you to set the call frequency of the broadcast messaging of audio-video group, which defaults to one message per second and can be set to up to five messages per second.

This feature is available only for Premium edition users. You can [click here to upgrade](#).

Audio-video group member banning

Once this feature is enabled, audio-video group members can be banned as needed. A banned member cannot receive group messages or rejoin the group during the ban.

Note

This feature is available only for native SDK v6.6 and web SDK v2.22 or later. If you are using an earlier SDK version, you need to upgrade your SDK before you can use the feature.

This feature is available only for Premium edition users. You can [click here to upgrade](#).

Message history for new members of an audio-video group

Message history for new members is an important feature to increase the user stickiness in audio-video groups. It enables users to know what was going on before they enter an audio-video group, so they can quickly fit into interactive discussions and feel more involved. This helps deliver an highly immersive live chat experience and increase users' length of stay in live rooms.

1. On the **Login and Message** page, click **Edit** in the upper-right corner of the **Message History for New Members** area.
2. In the pop-up dialog box, set the number of messages viewable to new members.
3. Click **Confirm**.

Read receipts for group messages

Group message read receipt is a must-have feature for efficient communication. As a powerful feedback tool, it allows viewing the numbers and details of members who have or have not read the sent messages. This helps teams create a more timely and efficient atmosphere of communication, especially in business and OA scenarios.

1. On the **Login and Message** page, click **Edit** in the upper-right corner of **Read receipts for group messages**.
2. In the pop-up **Read receipts for group messages** dialog box, set the group types that support message receipts.
3. Click **Confirm**.

Note

The group message read receipt feature is **available only for Premium edition users**. If you are not an Premium edition user, you need to [upgrade](#) before you can use the feature. The feature is supported by **native SDK v6.1.2155 or later** and is applicable to **work groups (Work)**, **public groups (Public)**, and **meeting groups (Meeting)** that support up to 200 members per group.

Account Management

Last updated : 2024-02-19 14:18:18

Log in to the [Chat console](#), click the target app card, and select **Account Management** in the left sidebar. You can manage accounts according to your business needs.

Creating an Account

1. On the **Account Management** page, click **Create account**.
2. Configure the following parameters in the pop-up dialog box:

Create account

Account Type

☒ General ☐ Admin ⓘ

Username *

Enter User ID

Nickname

Enter a nickname (optional)

Profile Photo

Enter the profile photo URL (optional)

Confirm

Cancel

Account Type: Select **General** or **Admin**. The role of app admin has the highest level of management permissions. It can call RESTful APIs to perform operations such as creating or disbanding a group, and sending messages to all members. Each app supports up to 10 admins.

Username: Enter the user ID. This field is required.

Nickname: Enter the nickname. This field is optional.

Profile Photo: Enter the URL to the user's profile photo. This field is optional.

3. Click **Confirm**.

After the account is created, you can see the account's username, nickname, type, profile photo, and creation time in the account list.

Deleting Accounts

1. On the **Account Management** page, select the accounts to delete and click **Batch Delete** above the account list.
2. In the pop-up dialog box, click **Confirm**. Data cannot be restored once deleted.

Are you sure you want to delete the selected accounts?

Selected accounts: 2 [Show More](#) ▼

Note that the accounts' data such as relationship chain and profile will **cannot be recovered**.

Confirm

Cancel

Editing an Account

1. On the **Account Management** page, locate the account to edit and click **Edit** in the **Operation** column.
2. Configure the following parameters in the pop-up dialog box:

Username: This field cannot be edited.

Nickname: You can edit the user's nickname. This field is optional.

Account Type: This field cannot be edited.

Gender: You can edit the user's gender. This field is optional.

Birth Date: You can edit the user's birthday. This field is optional.

Location: You can edit the location. This field is optional.

What's Up: You can edit the status. This field is optional.

Friend Request Verification: You can edit the friend request verification mode.

Language: You can edit the language. This field is optional.

Profile Photo: You can edit the profile photo. This field is optional.

Message settings: You can select message settings. This field is optional.

Friending: You can specify whether the admin prohibits the user from initiating a friend request. This field is optional.

Level: You can edit the level. This field is optional.

Role: You can edit the role. This field is optional.

3. Click **Confirm**.

Exporting Accounts

1. Single account export: On the **Account Management** page, locate the account to export and click **Export** in the **Operation** column.

<div>Create accountBatch ImportBatch Export</div>				
<input type="checkbox"/>	Username (UserID)	Nickname	Account Type ▾	Profile Photo
<input checked="" type="checkbox"/>	administrator		Administrator	2023-01-05 15:4
<input checked="" type="checkbox"/>	123		Ordinary Account	2023-02-01 16:4
<input type="checkbox"/>	111		Ordinary Account	2023-02-01 16:4
Total items: 3				

2. Batch export: On the **Account Management** page, select the accounts to export and click **Batch Export** above the account list.

Create account

Batch Delete

Batch Import

Batch Export

<div><div></div></div>	Username (UserID)	Nickname	Account Type ▾	Profile Photo	Creation time
<div><div></div></div>	1234		Administrator		2023-02-02 15:01:
<div><div></div></div>	administrator		Administrator		2022-12-30 16:31:
<div><div></div></div>	123		Ordinary Account		2023-02-02 15:00:
Total items: 3					

3. In the pop-up dialog box that reads **Export successful**, click **Download**.

Group Management

Last updated : 2024-02-07 17:33:31

Log in to the [IM console](#), click the target app card, and select **Group Management** in the left sidebar. You can manage groups according to your business needs.

Alternatively, you can call relevant RESTful APIs to manage groups. For more information, see the [Group Management API Documentation](#).

Adding Groups

1. On the **Group Management** page, click **Add Group**.

2. Configure the following parameters in the pop-up dialog box for adding a group:

Group Name: Enter the name of the group. This is a required parameter, and the length cannot exceed 30 bytes.

Group Owner ID: Enter the ID of the group owner. This is an optional parameter. You must enter the name of a registered user.

Group Type: Set the group type, which can be Work, Public, Meeting, or Audio-video Group. For more information on group types, see [Group Types](#).

3. Click **OK** to save the configuration.

After creating the group, you can view the group ID, group name, group owner, group type, and creation time of the group in the group list.

Viewing Group Details

On the **Group Management** page, you can click **View Details** in the row of the target group to go to the **Group Details** page, where you can view and modify the basic information of the group and manage group members.

Modifying basic information

1. On the **Group Details** page, click **Edit** in the basic information area.

2. In the pop-up dialog box for modifying group information, you can modify the group name and group introduction.

Modify Group Info

Group Name*

test

Group Info

Enter group info

Confirm

Cancel

3. Click **Confirm** to save the configuration.

Managing group members

Adding a group member

1. On the **Group Details** page, click **Add Member** in the group member management area.
2. In the pop-up dialog box for adding members, enter the username.

Note:

You must enter the name of a registered user.

Add Member

User ID*

Enter the user ID

Enter the registered user ID

Confirm

Cancel

3. Click **Confirm** to save the configuration.

After adding a group member, you can view the username, nickname, join time, last speak time, and role of the member on the group member list.

Deleting a group member

1. On the **Group Details** page, you can delete group members in the following ways:

Delete a single member: Click **Delete** in the row of the target member.

Delete a batch of members: Select the members to be deleted and click **Delete Members** above the group member list.

2. In the pop-up dialog box, click **Confirm**.

After deletion, the selected members will no longer belong to the group.

Sending Messages

1. On the **Group Management** page, you can send messages in the following ways:

Send a message to a single group: Click **Send Messages** in the row of the target group.

Send a message to multiple groups: Select the target groups to which you want to send a message and click **Send Messages** above the group list.

2. In the pop-up dialog box for sending a group message, enter the message content.

Note:

The message length cannot exceed 300 characters.

3. Click **OK** to send the message.

Deleting Groups

After a group is deleted, all its information will be deleted and cannot be recovered. Please exercise caution when deleting groups.

1. On the **Group Management** page, you can delete groups in the following ways:

Delete a single group: Click **Delete** in the row of the target group.

Delete a batch of groups: Select the target groups to be deleted and click **Delete Groups** above the group list.

2. In the pop-up dialog box, click **Confirm**.

After the group is deleted, all its information will be deleted and cannot be recovered.

Webhook Configuration

Last updated : 2024-02-07 17:33:32

Log in to the [IM console](#), click the target app, and select **Webhook Configuration** in the left sidebar. You can configure webhook URLs and decide which webhooks to enable according to your business needs.

Configuring Webhook URLs

1. On the **Webhook Configuration** page, click **Edit** in the webhook URL configuration area.
2. In the webhook URL configuration dialog box that pops up, enter the webhook URL.

Note:

The webhook URL must start with `http://` or `https://`.

If you have not yet applied for a domain name, you can directly configure an IP address, for example,

```
http://123.123.123.123/imcallback .
```

Only letters (`a-z` , case-insensitive), numbers (0-9) and hyphens (-) can be used. Spaces and the following characters are not supported: `!$&?`.

The hyphen (-) cannot appear consecutively, be registered independently, or be placed at the beginning or end.

The length of the domain name cannot exceed 63 characters.

The webhook URL of IM uses ports 80/443 by default. When the webhook URL is replaced, port changes are involved. Please avoid the situation where the ports before and after the replacement are mutually prefixed; for example, avoid changing `https://xxx:443` to `https://xxx:4433` or changing `https://xxx` to `https://xxx:4433`.

3. Click **OK** to save the configuration.

Configuring Event Webhooks

1. On the **Webhook Configuration** page, click **Edit** in the webhook configuration area.
2. In the webhook configuration dialog box that pops up, check the desired webhooks.

Event Callback Configuration

Group

☐ Callback after group creation

☐ Callback after member leaving a group

☐ Callback after member entering a group

☐ Callback after speaking in a group

☐ Callback before application to enter a group

☐ Callback before group creation

☐ Callback before adding a member to a group

☐ Callback before speaking in a group

☐ Callback after disbanding groups

☐ Callback after group is full

Callback after group profile modification

☐ Callback after group portrait URL change

☐ Callback after group info modification

☐ Callback after group name change

☐ Callback after modifying group notice

Info Relationship Chain

☐ Callback after adding users to blocklist

☐ Callback after friend adding

☐ Callback after removing users from blocklist

☐ Callback after friend deletion

One-to-One Message

☐ Callback before sending one-to-one messages

☐ Callback after sending one-to-one messages

Online Status

☐ Online status change callback

Confirm

Cancel

3. Click **Confirm** to save the configuration.

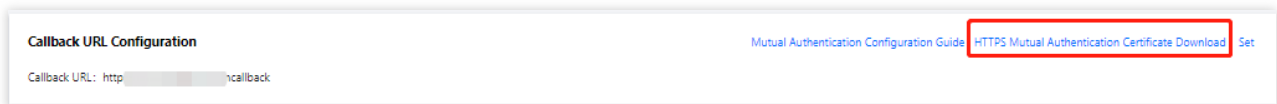
Downloading an HTTPS Mutual Authentication Certificate

After configuring webhook URLs, you can download an HTTPS mutual authentication certificate from the console for future use.

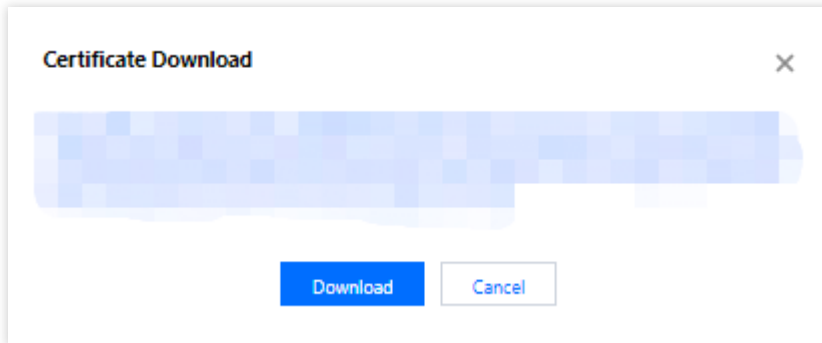
Note:

You can configure mutual authentication based on your actual needs. For the detailed configuration methods, see [Mutual Authentication Configuration](#).

1. Go to the [console](#), open the [Webhook Configuration](#) page, and click **HTTPS Mutual Authentication Certificate Download** in the webhook URL configuration area in the upper-right corner.



2. In the certificate download dialog box that pops up, click **Download**.



3. Save the certificate file.

Subsequent Operations

After configuring webhook URLs and enabling the corresponding event webhooks, you can refer to [Webhooks](#) to use the corresponding webhooks in order to obtain user and operation information in real time.

Statistics

Last updated : 2024-02-07 17:33:31

The Chat console provides you with data statistics and analysis features. You can log in to the [Chat console](#), click the target app card, and choose **Monitoring Dashboard** in the left sidebar to view app data such as user base, message activity, group size, and real-time monitoring data.

Note:

Normally, the data is updated at 10:00 every morning. In the event that the data is 0 or not updated, check whether the SDKAppID produced relevant data (for example, whether there are new registered users) in the specified period. If data was produced but not updated, just wait a while for it to be updated.

Daily Statistics

User base

1. On the **Daily Statistics** page, click the **User Base** tab.

2. In the overview area, you can view the following data:

Peak DAU of the current month: the peak DAU of the current month as of yesterday. This data is 0 on the first day of every month.

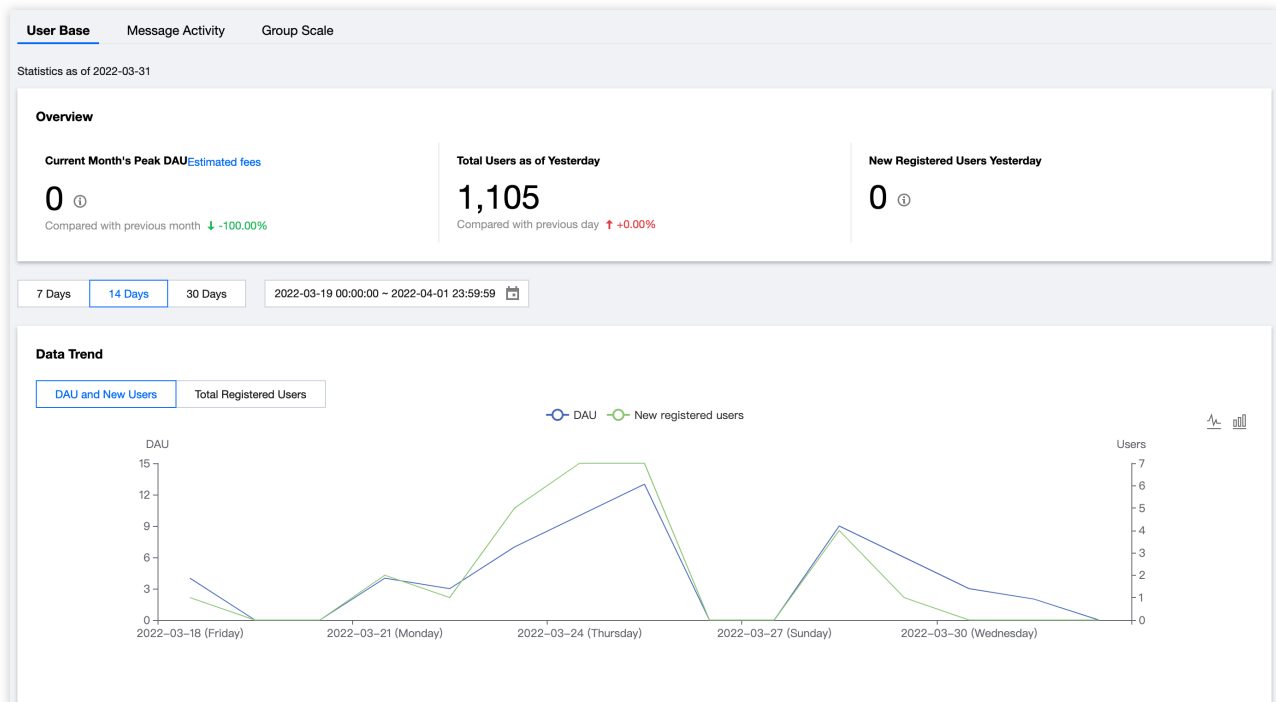
Cumulative number of users as of yesterday: the cumulative number of UserIDs registered with the SDKAppID as of yesterday.

Number of new registered users yesterday: the number of new UserIDs registered with the SDKAppID yesterday.

3. Select 7 days, 14 days, or 30 days, or specify a period.

4. In the data trend area, you can view the **DAU and New Users** or **Total Registered Users** chart for the selected period.

5. In the data details area, you can view the data of each day for the selected period, including DAU, DAU (day-over-day), total users, total users (day-over-day), new registered users, and new registered users (day-over-day). You can also export these data by clicking **Export as CSV**.



Message activity

1. On the **Daily Statistics** page, click the **Message Activity** tab.

2. In the overview area, you can view the following data:

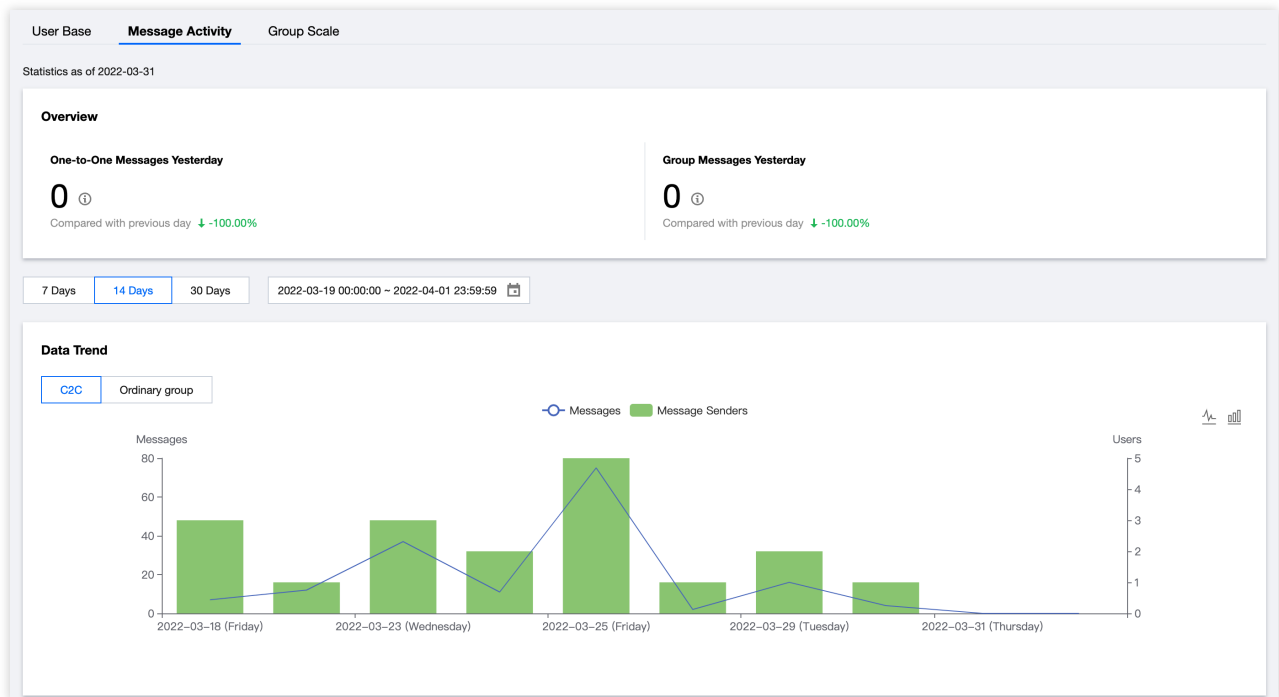
Number of one-to-one messages yesterday: the total number of C2C chat upstream messages under the SDKAppID yesterday.

Number of group messages yesterday: the total number of upstream messages in private group, public group, and chat room chats under the SDKAppID yesterday.

3. Select 7 days, 14 days, or 30 days, or specify a period.

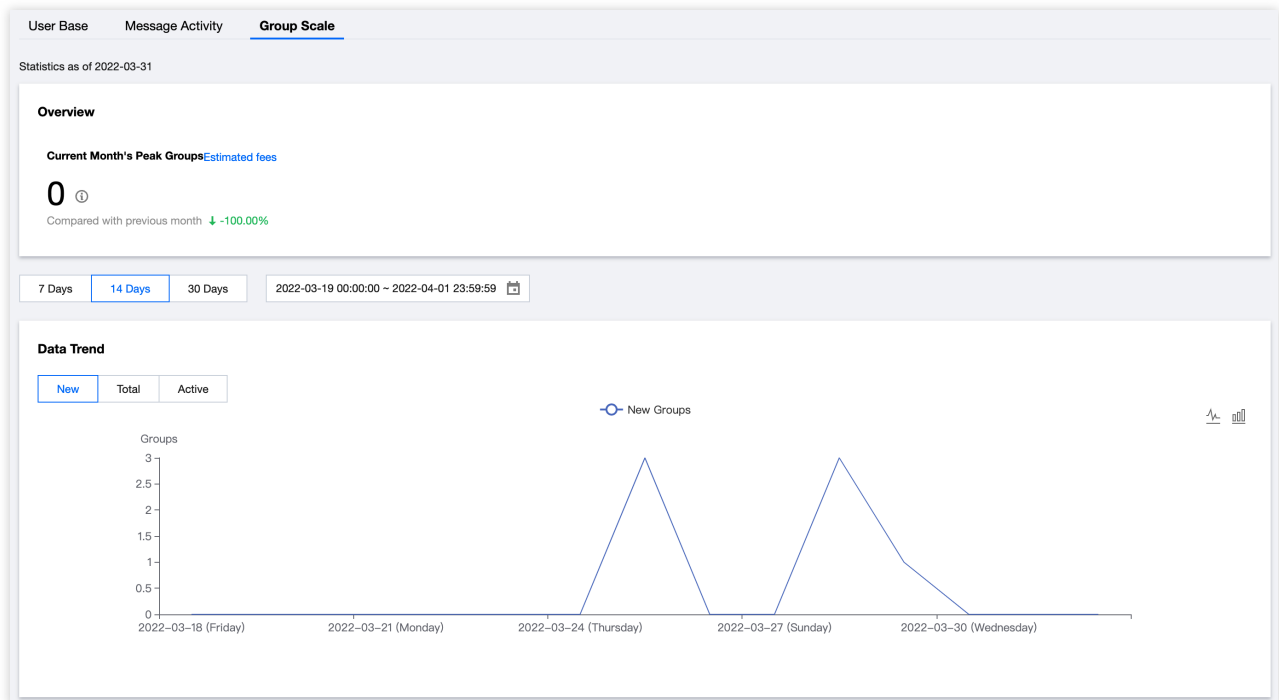
4. In the data trend area, you can view the **C2C** or **Ordinary Group** message count charts for the selected period.

5. In the data details area, you can view the data of each day for the selected period, including message count, message count (day-over-day), message senders, message senders (day-over-day), offline pushes, and offline pushes (day-over-day). You can also export these data by clicking **Export as CSV**.



Group size

1. On the **Daily Statistics** page, click the **Group Scale** tab.
2. In the overview area, you can view the **Current Month's Peak Groups** data, which is the peak group count of the current month as of yesterday under the SDKAppID. This is 0 on the first day of every month.
3. Select 7 days, 14 days, or 30 days, or specify a period.
4. In the data trend area, you can select a data item to view the trends of **New**, **Total**, or **Active** groups within the selected time range.
5. In the data details area, you can view the data in each day for the selected period, including new groups, new groups (day-on-day), active groups, active groups (day-on-day), peak group count, and peak group count (day-on-day). You can also export these data by clicking **Export as CSV**.



Real-Time Monitoring

Note:

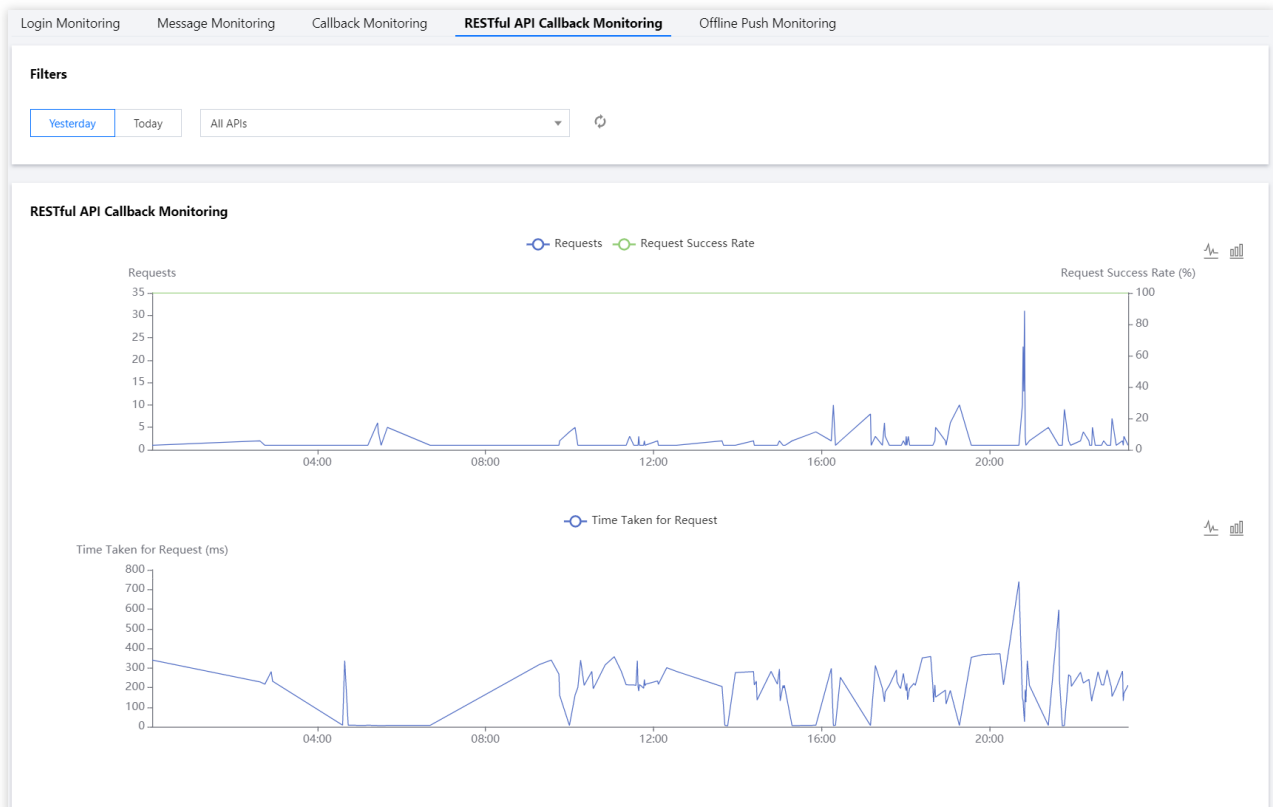
The real-time monitoring feature is in beta testing and is still being updated in iteration mode. If you have any feedback or suggestions, [submit a ticket](#).

1. In the left sidebar, choose **Monitoring Dashboard > Real-Time**.
2. In the overview area, you can view **Current Online Users**, **One-to-One Messages Today**, **Ordinary Group Messages Today**, and **Audio-Video Group Messages Today**.
3. In the detailed monitoring data area, data of the 24 hours of the natural day is displayed on the timestamp by default. When the mouse cursor points to the data chart area, you can use the scroll wheel to zoom in the timestamp to view details, drag the timestamp left and right to view the data before and after the time, and click the legend below the timestamp to hide or show the corresponding value in the chart.

In the login monitoring area, you can view the login times and login success rate of each client.

Note:

Currently, only the login data reported by 4.8.10 or later Chat SDKs for iOS, Android, Windows, and macOS will be displayed. You are advised to upgrade to the [latest version of SDK](#).



In the message monitoring area, you can view the number of one-to-one or group messages sent by each client and the message sending success rate.

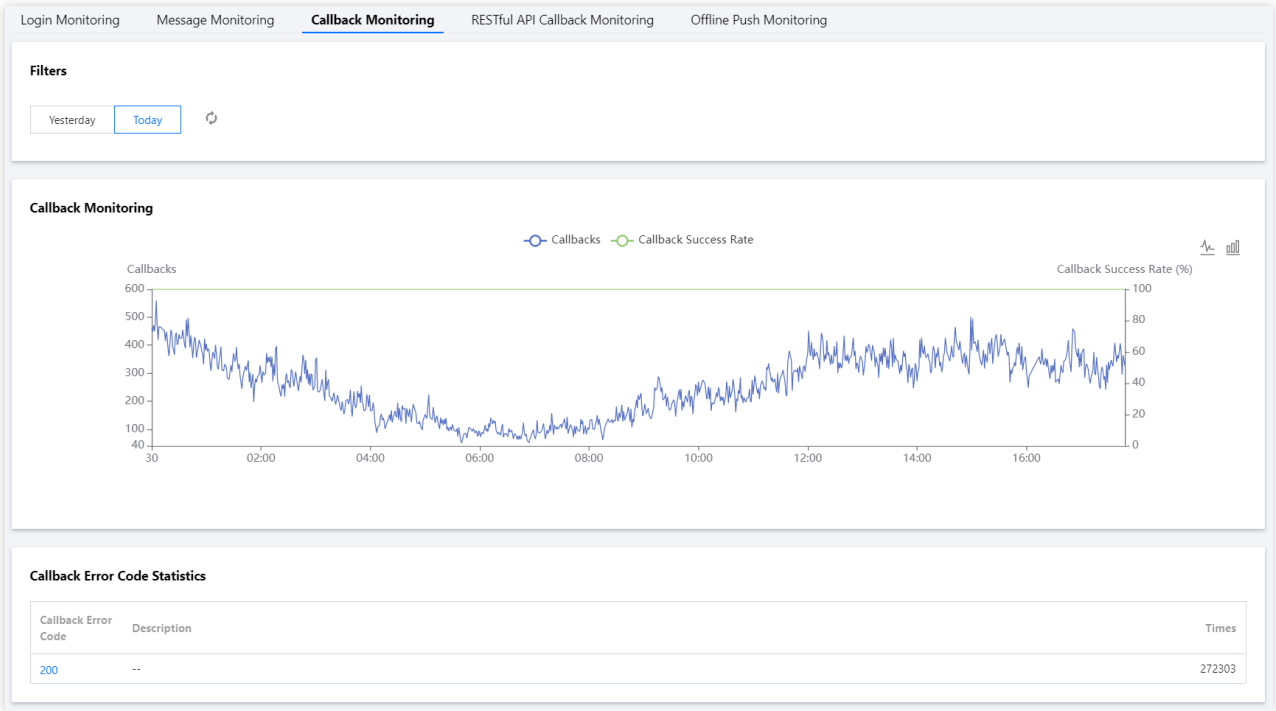
Note:

Currently, only the login data reported by 4.8.10 or later Chat SDKs for iOS, Android, Windows, and macOS will be displayed. You are advised to upgrade to the [latest version of SDK](#). Currently, the web SDK does not support collecting message statistics by chat type.

In the callback monitoring area, you can view the number of callbacks and the callback success rate.

In the RESTful API monitoring area, you can view the number of RESTful API requests and the request success rate.

In the offline push monitoring area, you can view the number of offline push times and the push success rate.



Auxiliary Development Tools

Last updated : 2024-02-07 17:33:32

Offline Push Check

Offline push issue locator

This tool allows you to query issues related to the failure to receive offline messages.

1. Log in to the [Chat console](#) and click the target Chat app section.
2. In the left sidebar, choose **Auxiliary Tools > Push Message Tool**.
3. In the **Offline Push Issue Locator** area, enter the UserID.
4. Click **Obtain Device Status** to view the uploaded information for the UserID, such as the certificate ID and device token.

Note

If no UserID information, such as the certificate ID and device token, has been uploaded, the query ends.

5. Select any certificate ID of the UserID, click **Start Checking**, and then view the sending result.

If a success prompt is displayed, the certificate information you entered in the console is correct and the token was uploaded by calling the SDK API. You can use the [user status checker](#) for further troubleshooting.

If a failure prompt is displayed, you can view the cause of the failure and the solution.

Offline Push Issue Locator

[What is offline p](#)

This tool is used for self-service checking when offline pushes cannot be received.

Enter the username (UserID)

Get Device Info

Certificate ID

Select certificate ▼

Start Checking

Results:

User status checker

This tool automatically obtains the user's client status and checks whether the user is ready to receive offline push messages.

1. Log in to the [Chat console](#) and click the target Chat app section.
2. In the left sidebar, choose **Auxiliary Tools > Push Message Tool**.
3. In the **User Status Checker** area, enter the UserID.
4. Click **Get Status** to view information such as the current status and client type of the UserID.

If you are prompted that the UserID is ready to receive offline push messages, you can log in with a different UserID on another device to send one-to-one text messages to the current UserID to check whether it can receive the messages.

User Status Checker

This tool is used to automatically obtain user's client status and check whether the user can receive offline pushes.

Enter the username (UserID)

Get Status



Users cannot receive offline pushes when they are not logged in (the Offline state). In addition, Android users can receive offline pushes only when they are in PushOnline state; iOS users can receive offline pushes only when their clients work in background.

UserSig Generation and Verification

Signature (UserSig) generator

The system automatically obtains the key of the current app. After entering the UserID, you can use this tool to quickly generate a signature (UserSig) to run through demos and debug features locally. If you need to generate a UserSig for online services, see [Generating UserSig on the Server](#).

1. Log in to the [Chat console](#) and click the target Chat app section.
2. In the left sidebar, choose **Auxiliary Tools > UserSig Tools**.
3. In the Signature (UserSig) Generator area, enter the UserID.
4. Click **Generate UserSig** to generate a signature, which expires after 180 days.
5. Click **Copy UserSig** to copy the signature and then paste and save the signature.

Signature (UserSig) Generator

This tool can quickly generate a UserSig, which can be used to run through demos and to debug features.

Enter the username (UserID)

Key

```
335105403a1ca03f*****faec0b940354c1f0
```

Generate UserSig

The generated UserSig is :

```
eJwt  
GaH  
5N  
qL2  
-
```

Copy UserSig

Signature (UserSig) verification tool

The system automatically obtains the key of the current app. After entering the UserID and UserSig, you can use the tool to quickly check the validity of the UserSig.

1. Log in to the [Chat console](#) and click the target Chat app section.
2. In the left sidebar, choose **Auxiliary Tools > UserSig Tools**.

3. In the Signature (UserSig) Verifier area, enter the UserID and UserSig.

Signature (UserSig) Verifier

This tool is used to verify the validity of the UserSig you use.

Enter the username (UserID)

Key

335105403a1ca03f*****faec0b940354c1f0

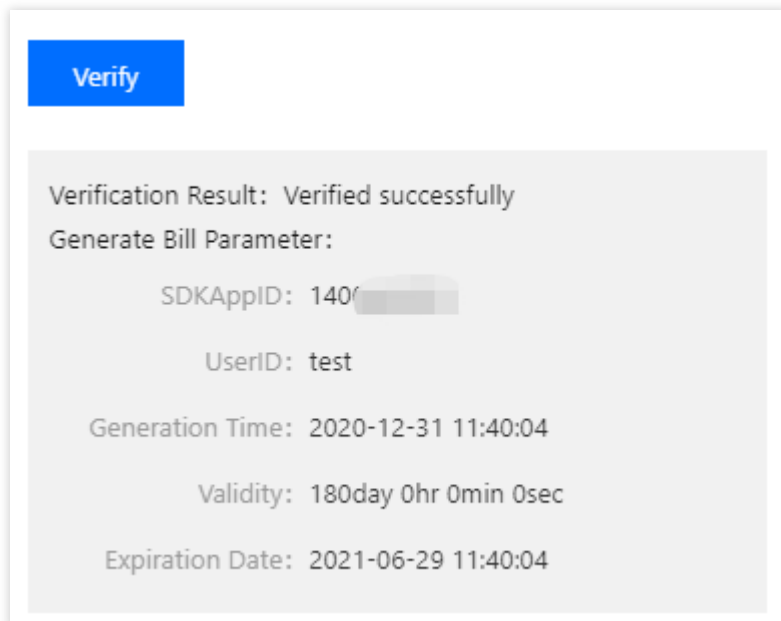
UserSig

eJwtzM
ISUvOtdOdtqif5*jSJp2Ad8fz7kwlg__

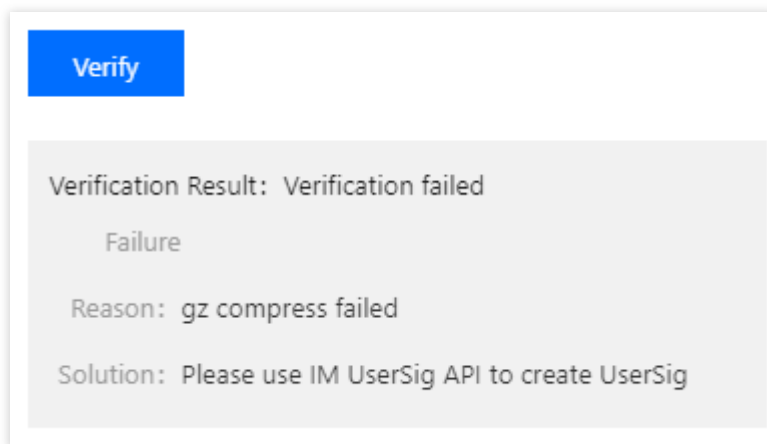
Verify

4. Click **Verify** to see the verification result.

If verification succeeds, you can view the SDKAppID, UserID, generation time, service time, and expiration time of the UserSig in the verification results.



- If verification fails, you can view the cause of failure and solution in the verification results.



Self-Troubleshooting Logs

Tencent Cloud Chat console provides self-troubleshooting feature to allow developers to query the backend log information of Chat in the last three days to quickly locate and solve issues.

1. Log in to the Chat console, click the target Chat app section.
2. In the left sidebar, choose **Auxiliary Tools > Self-Troubleshooting Logs**.
3. Configure following filters to query logs:

Event name (Optional): Select events for querying.

UserID (Optional): Enter username (UserID), which is the UserID of the message sender.

Receiver/Group ID (Optional): Enter target conversation ID. For a one-to-one chat, it is the userID of the message receiver. For a group chat, it is the GroupID of the group.

Error codes (Optional): Enter error codes. For error code descriptions, see [Error Codes](#).

Time range (Required): Select the time range of logs to be queried. Logs in the last three days can be queried.

4. Click **Query** to view the filtered logs.

Access Management

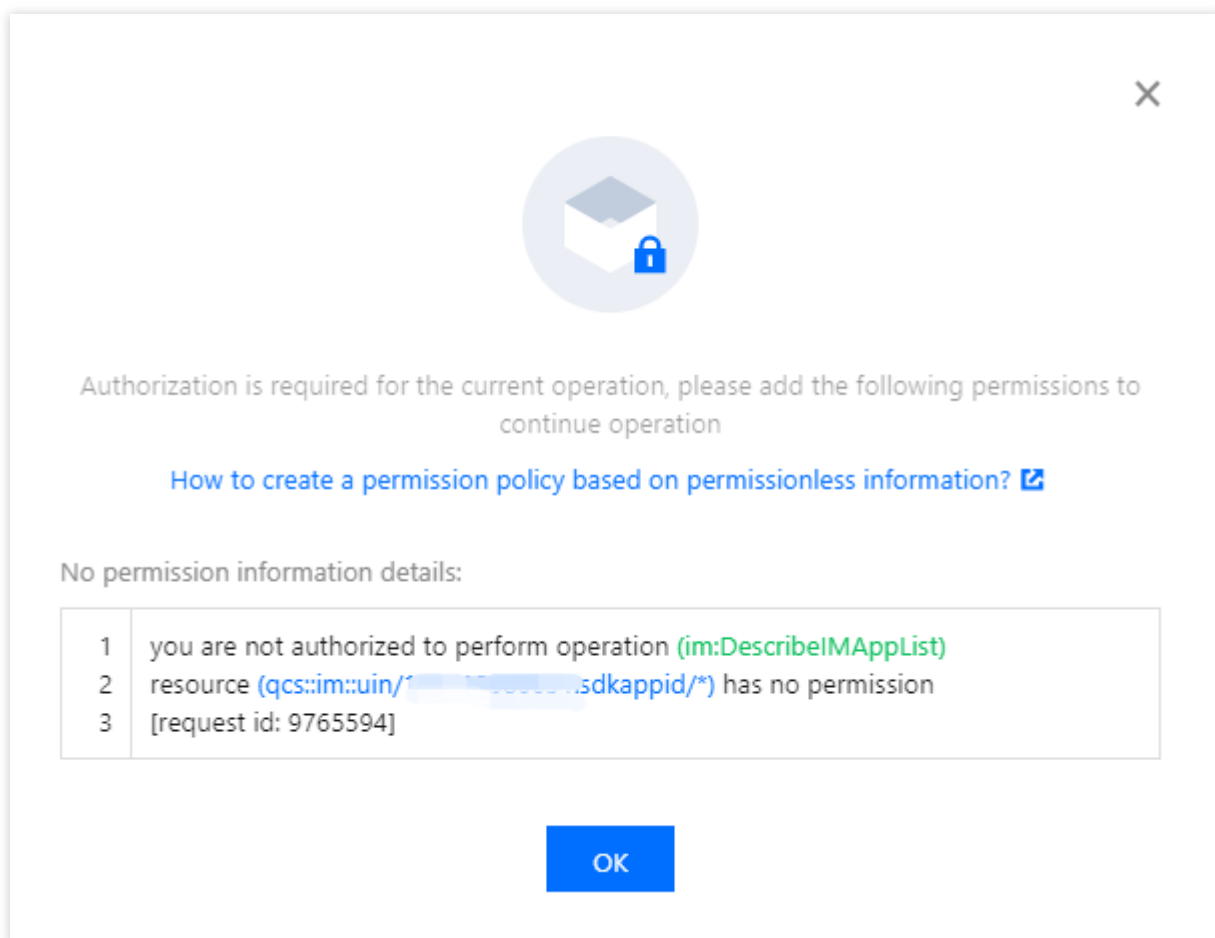
Granting Console Operation Permissions to Sub-accounts

Last updated : 2024-02-07 17:33:32

Overview

This document describes two authorization methods to resolve the following issues. Detailed steps are as below. To configure more complex permission policies, see [Custom Policy](#).

When you are using the IM service with a sub-account, the root account needs to authorize the sub-account to access the [IM console](#) and to configure settings. Otherwise, the console will not display the application list, as shown below:

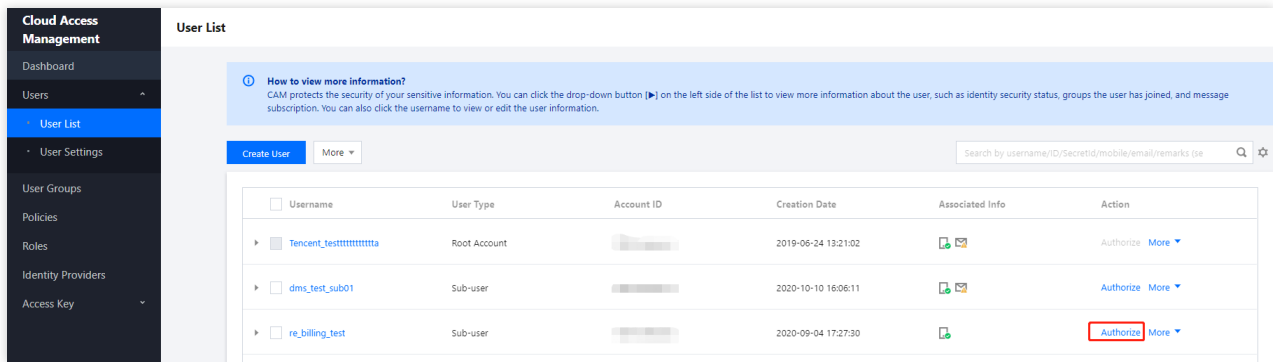


When a sub-account has access to tags, but it does not match its access to the console application tags, the sub-account cannot view the newly created applications.

Solution 1. Global Authorization

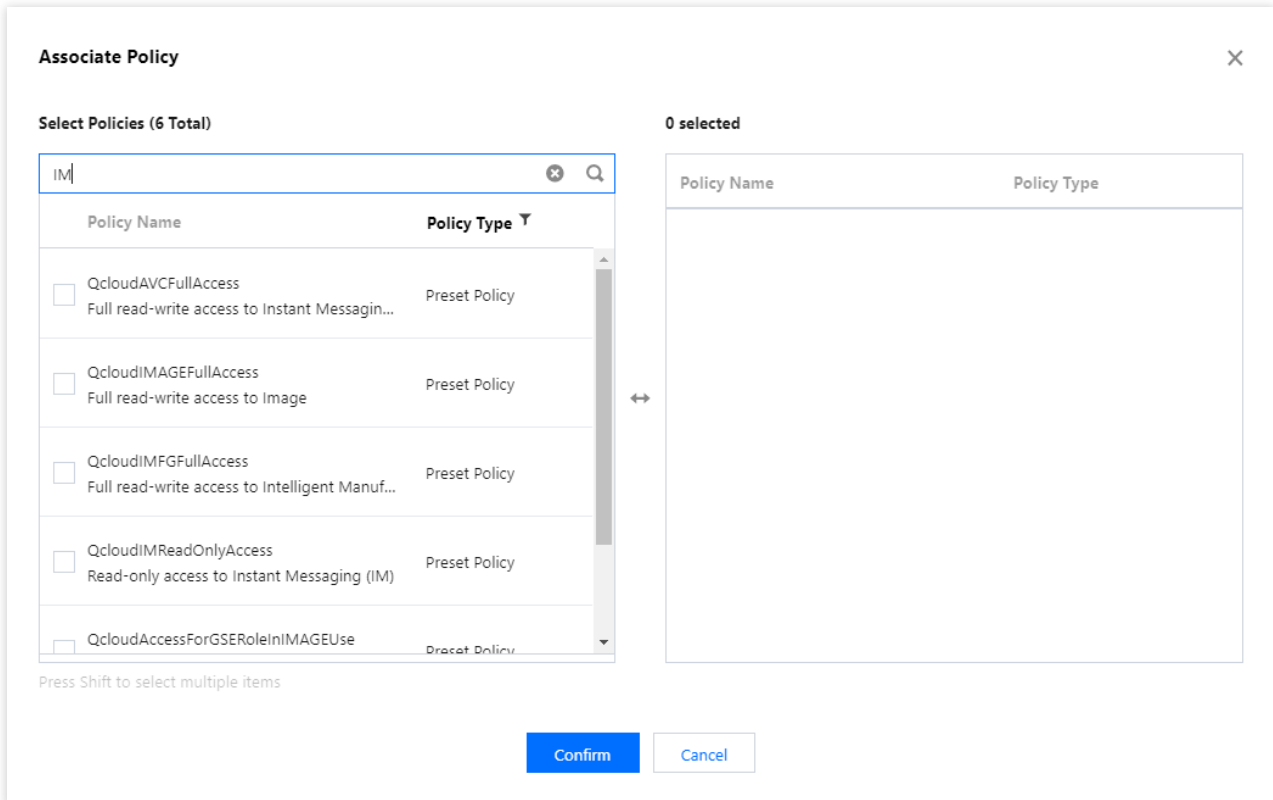
Step 1. Go to CAM to authorize

Log in to the [CAM console](#) using the root account, go to **User List**, click **Authorize** on the left of the sub-user, and the **Associate Policy** dialog box will pop up.



Step 2. Select policies

Search by **IM**, select the desired policies, and click **Confirm** to complete the authorization.



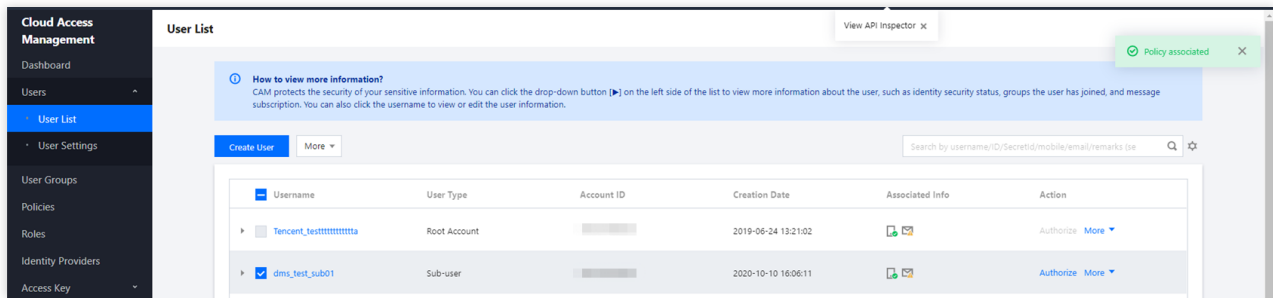
Note:

Read/write access: Allows users to access the console and modify configurations.

Read-only access: Allows users to access the console only, not to perform other operations.

Step 3. Complete authorization

If **Policy associated** is prompted in the upper right corner, the authorization is completed.



Solution 2. Authorization by Tag

This solution is designed for customers who need to authorize and manage sub-accounts by tag. Sub-accounts can only access and operate applications under the authorized tags.

Caution:

After a tag policy is assigned to a sub-account, the sub-account cannot access or operate applications with no tags. For a sub-account, there are no tags in a newly created application in the [IM console](#). Therefore, the root account needs to change the application tags to authorized tags so that the sub-account can use the application.

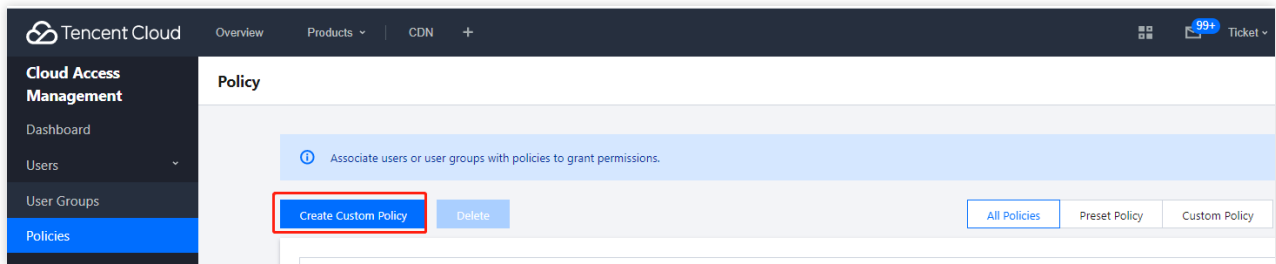
If you want to grant a sub-account the access to an existing app by tag, make sure you have configured tags for the app; otherwise, you will be unable to authorize by tag.

If no tags are configured for the app, go to the [Basic Configuration](#) page in the IM console to configure. For more information, see the **Configuring Tags** section in [Basic Configuration](#).

You can also go to [Tag List](#) to bind multiple apps to a tag at a time. For more information, see the **Binding resources** section in [Creating Tags and Binding Resources](#).

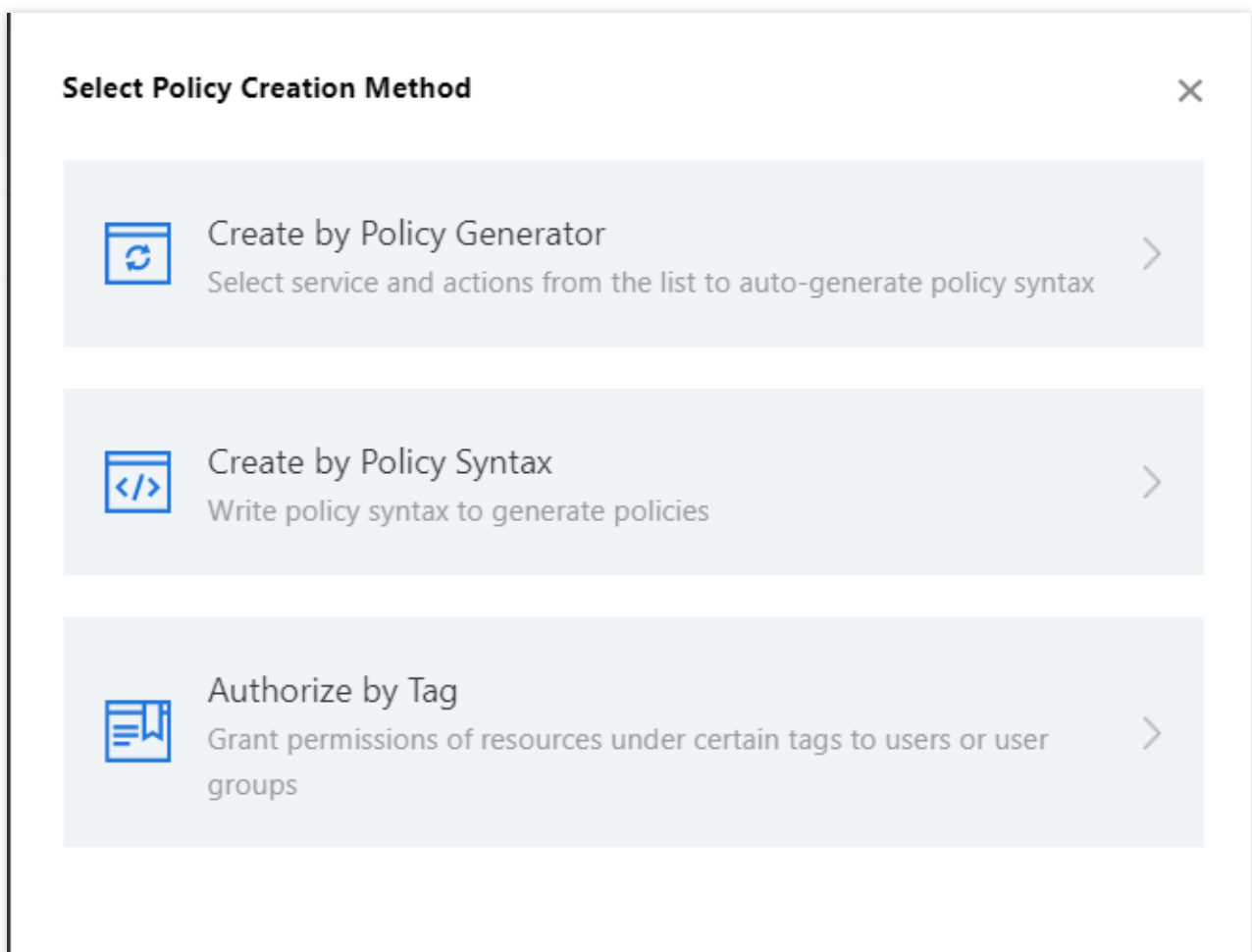
Step 1. Go to CAM to authorize

Log in to the [CAM console](#) using the root account, click **Policies > Create Custom Policy**, and the **Select Policy Creation Method** dialog box will pop up.



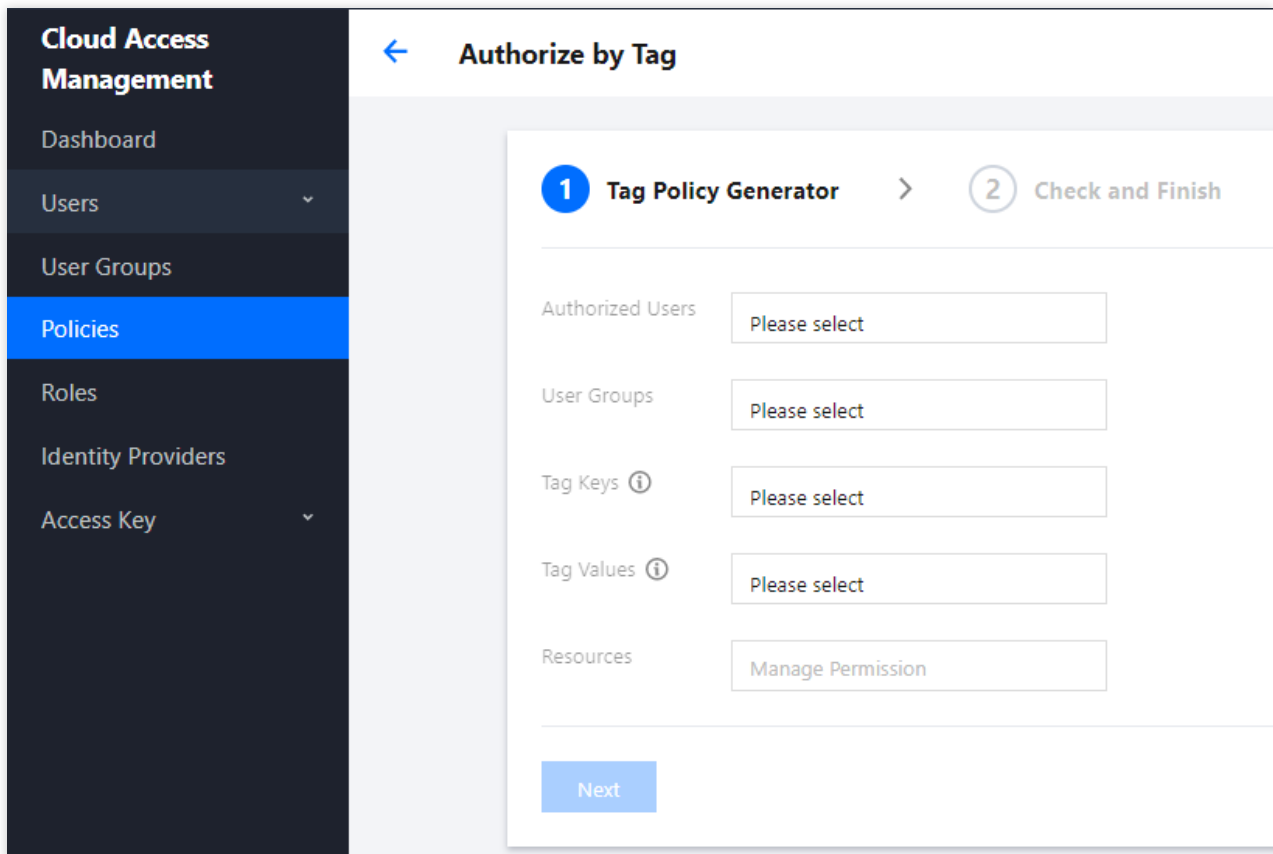
Step 2. Select a tag

Select **Authorize by Tag** to go to **Tag Policy Generator**.

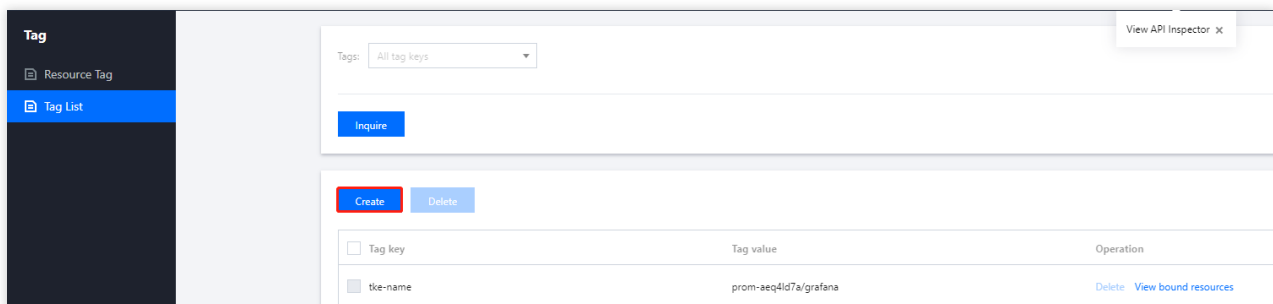


Step 3. Generate a policy

Enter the sub-account to authorize, tag, and other information in **Tag Policy Generator** and click **Next** to go to the next step.

**Note:**

If there are no tags, you need to log in to the [Tag console](#) to create a tag.

**Step 4. Complete authorization**

After confirming the information is correct, click **Done** to complete the authorization.

Cloud Access Management

Dashboard

Users

User Groups

Policies

Roles

Identity Providers

Access Key

← Authorize by Tag

1 Tag Policy Generator

2 Check and Finish

Policy Name *

policygen-20210205095508

Authorized Users

Tencent_testttttttttta

Authorized User Groups

test2

Policy Content

```
1 {
2   "version": "2.0",
3   "statement": [
4     {
5       "effect": "allow",
6       "action": "*",
7       "resource": "*",
8       "condition": {
9         "for_any_value:string_equal": {
10          "qcs:tag": [
11            "tke-lb-serviceuid&4663ccfc-bb6f-4492-93b7-5c7c345fb311"
12          ]
13        }
14      }
15    ]
16  }
17 }
```

Back

Done

Preset Policy

Last updated : 2024-02-07 17:33:32

Caution:

This document describes the Cloud Access Management (CAM) feature for IM. For more information on CAM for other Tencent Cloud services, see [CAM-Enabled Products](#).

Essentially, IM CAM binds sub-accounts to policies or grants policies to sub-accounts. You can use preset policies in the console for simple authorization operations. For more information on complicated authorization operations, see [Custom Policies](#).

The table describes the preset policies provided by IM.

Policy	Description
QcloudAVCFullAccess	IM read and write permissions
QcloudIMReadOnlyAccess	IM read-only permission

Preset Policy Usage Example

Creating a sub-account with IM permissions

1. Log in to the [User List](#) page in the CAM console with the [root account](#). Then, click **Create User**.
2. On the **Create User** page, click **Custom Create** to go to the **Create Sub-user** page.

Note:

For information on the operations that you must perform before configuring user permissions, see [Creating Sub-user](#).

3. On the **User Permissions** page:

- (1) Search for and select the `Instant Messaging` preset policy.
- (2) Click **Next**.

4. Click **Complete** in the **Review** column. After the sub-user is created, record the login link, download the security credentials, and store them properly. The table describes the relevant information.

Information	Source	Function	Required
Login link	Copied on the page	Facilitate console login and skip the root account entry step	No
Username	Security credential CSV file	Entered when you log in to the console	Yes

Password	Security credential CSV file	Entered when you log in to the console	Yes
SecretId	Security credential CSV file	Used when a server API is called. For more information, see Access Key	Yes
SecretKey	Security credential CSV file	Used when a server API is called. For more information, see Access Key	Yes

o5. Provide the authorized party with the preceding login link and security credentials. The authorized party can then use the sub-account to perform IM operations, including accessing the IM console and calling IM server APIs.

Granting IM permissions to an existing sub-account

1. Log in to the [User List](#) page in the CAM console with the [root account](#). Then, click the sub-account to authorize.
2. On the **User Details** page, click **Add Policy**. If the sub-account already has permissions, click **Associate Policy**.
3. Select **Select policies from the policy list**, search for and select the `Instant Messaging` preset policy and complete the authorization process as instructed.

Deleting IM permissions from a sub-account

1. Log in to the [User List](#) page in the CAM console with the [root account](#). Then, click the sub-account from which you want to delete permissions.
2. On the **User Details** page, find the `Instant Messaging` preset policy, and click **Unassociate** for the policy. Then, complete the deauthorization process as instructed.

Custom Policy

Last updated : 2024-02-07 17:33:32

Caution:

This document describes the Cloud Access Management (CAM) feature for IM. For more information about CAM for other Tencent Cloud services, see [CAM-Enabled Products](#).

You can easily use [preset policies](#) in the CAM console for authorization. However, preset policies only provide coarse-grained permission control and cannot be refined to IM applications and [Tencent Cloud APIs](#). If you need refined permission control, you must create custom policies.

Custom Policy Creation Methods

The table compares several custom policy creation methods with detailed instructions for using them.

Entry	Method	Effect	Resource	Action	Flexibility	Difficulty
CAM console	Policy generator	Manual selection	Syntax description	Manual selection	Medium	Medium
CAM console	Policy syntax	Syntax description	Syntax description	Syntax description	High	High
CAM server API	CreatePolicy	Syntax description	Syntax description	Syntax description	High	High

Note:

IM does not support custom policy creation by product feature or project.

Manual selection indicates that you must select an object from the option list in the console.

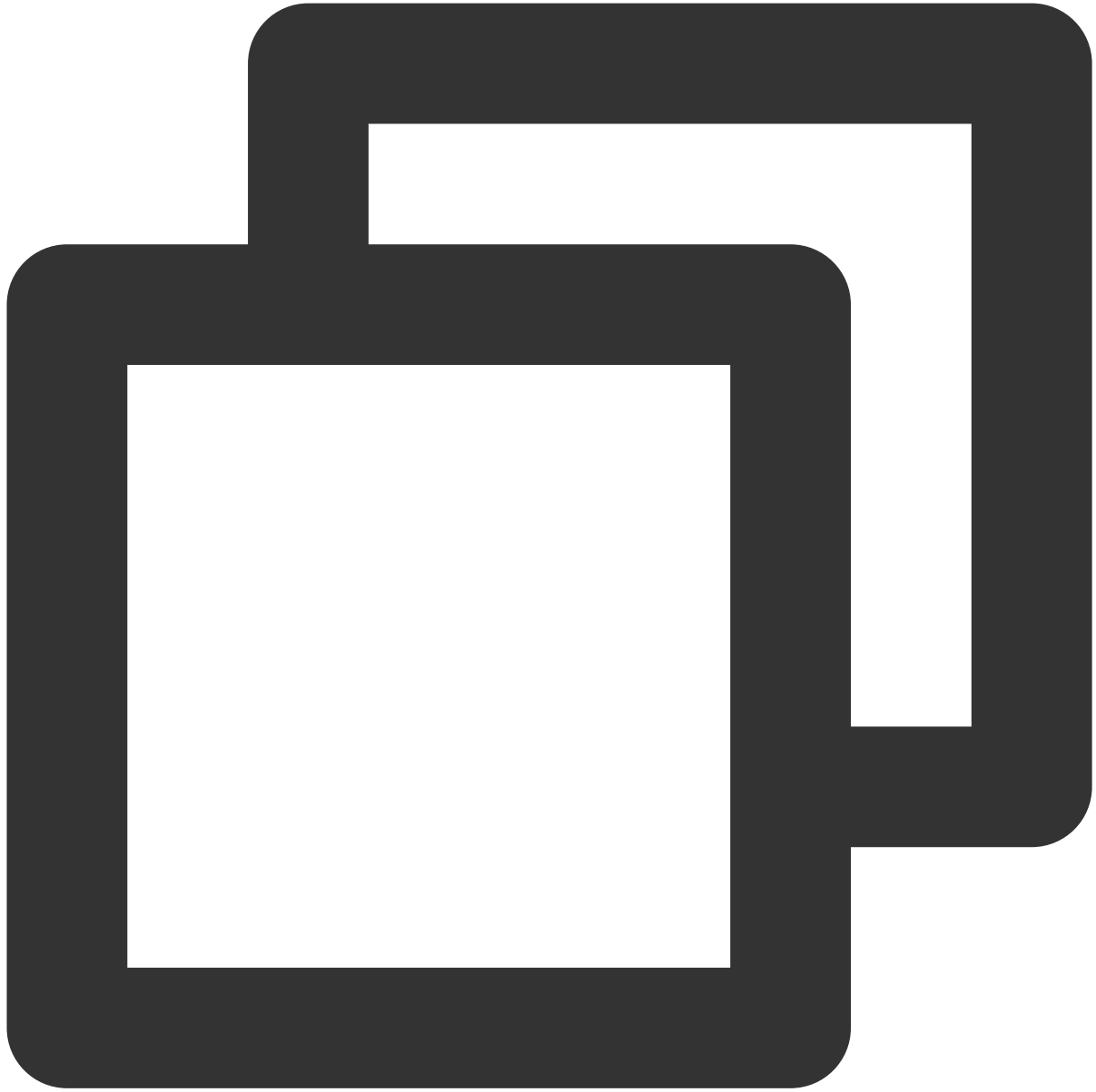
Syntax description indicates that the [authorization policy syntax](#) is used to describe objects.

Authorization Policy Syntax

Resource syntax description

As mentioned previously, the resource granularity for IM permission management is applications. Policy syntax description of applications comply with the [Resource Description Method](#). In the following example, the developer's root account ID is 12345678, and the developer creates three applications whose SDKAppIDs are 1400000000, 1400000001, and 1400000002 respectively.

Policy syntax description for all IM applications



```
"resource": [  
  "qcs::im::uin/12345678:sdkappid/*"  
]
```

Policy syntax description for a single application



```
"resource": [  
  "qcs::im::uin/12345678: sdkappid/1400000001"  
]
```

Policy syntax description for multiple applications

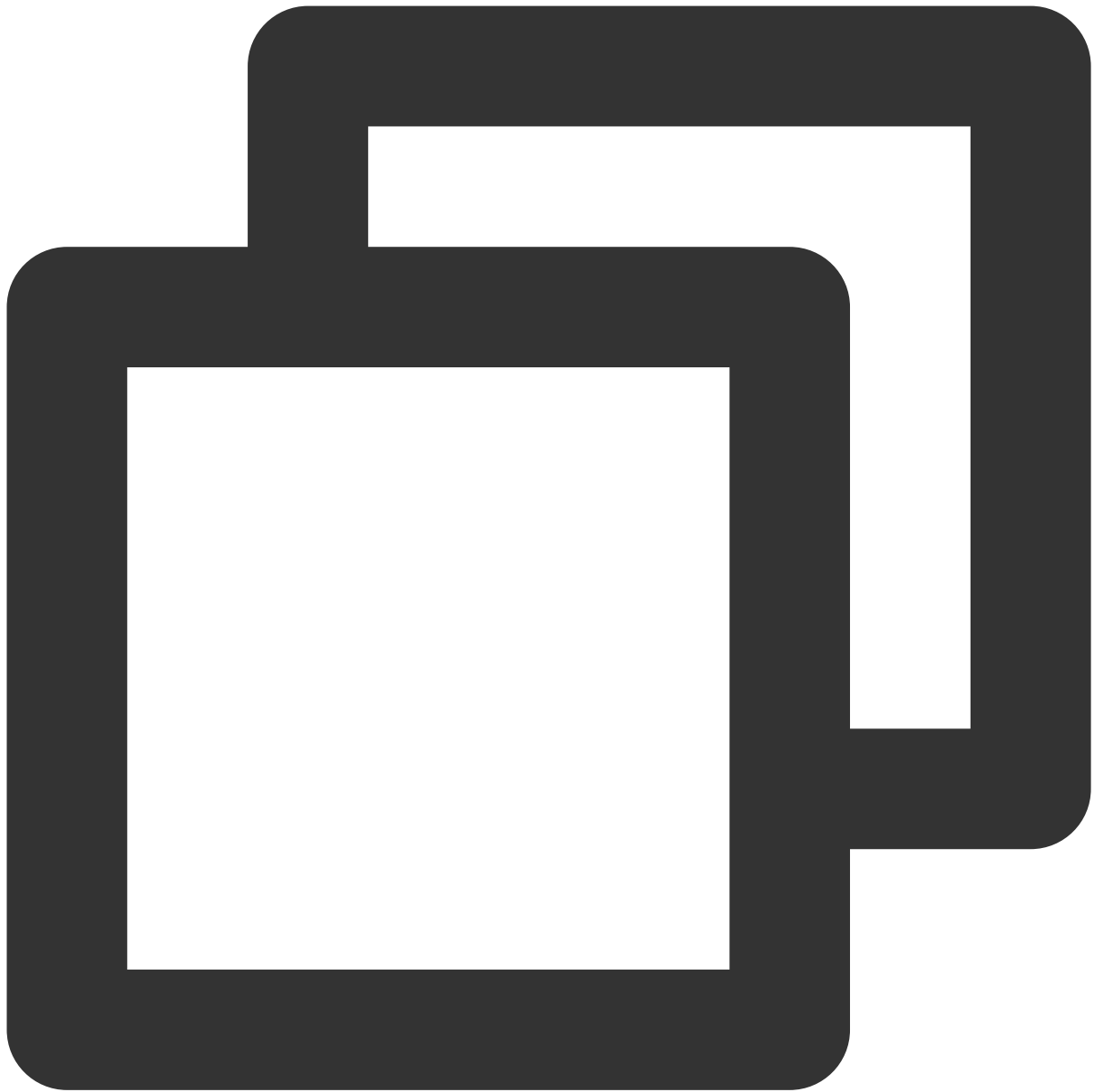


```
"resource": [  
  "qcs::im::uin/12345678: sdkappid/1400000000",  
  "qcs::im::uin/12345678: sdkappid/1400000001"  
]
```

Action syntax description

As mentioned previously, the action granularity of TRTC permission management is Tencent Cloud APIs. In the following example, Tencent Cloud APIs such as `DescribeAppStatList` (for obtaining the application list) and `DescribeSdkAppInfo` (for obtaining application information) are used.

Policy syntax description for all Tencent Cloud APIs for IM



```
"action": [  
  "name/im:*"  
]
```

Policy syntax description for a single Tencent Cloud API



```
"action": [  
  "name/im:DescribeAppStatList"  
]
```

Policy syntax description for multiple Tencent Cloud APIs



```
"action": [  
  "name/im:DescribeAppStatList",  
  "name/im:DescribeTrtcAppAndAccountInfo"  
]
```

Custom Policy Usage Example

Using the policy generator

In the following example, we will create a custom policy that allows all operations on the IM application whose SDKAppID is 1400000001.

1. Log in to the [Policies](#) page in the CAM console with the [root account](#). Then, click **Create Custom Policy**.

2. Select **Create by Policy Generator** to go to the policy creation page.

3. In the **Select Service and Action** step:

Select **Allow** for **Effect**.

Select **IM** for **Service**.

Select all items for **Action**.

Enter `qcs::im::uin/12345678:sdkappid/1400000001` for **Resource** based on the [resource syntax description](#).

Condition is optional.

Click **Add Statement**. A statement that allows all operations for the IM application 1400000001 appears.

4. Continue to add another statement on the same page by configuring the following settings:

Select **Deny** for **Effect**.

Select **IM** for **Service**.

Select `RemoveUser` for **Action**. (You can quickly find `RemoveUser` with the search feature.)

Enter `qcs::im::uin/12345678:sdkappid/1400000001` for **Resource** based on the [resource syntax description](#).

Condition is optional.

Click **Add Statement**. A statement that rejects the `RemoveUser` operation for IM application 1400000001 appears.

5. Click **Next** and rename the policy as needed (You can also retain the current policy name).

6. Click **Done**.

The method for granting the policy to other sub-accounts is the same as [Granting IM Permissions to an Existing Sub-account](#).

Using the policy syntax

In the following example, we will create a custom policy that allows all operations for the IM applications whose SDKAppIDs are 1400000001 and 1400000002.

1. Log in to the [Policies](#) page in the CAM console with the [root account](#). Then, click **Create Custom Policy**.

2. Select **Create by Policy Syntax** to go to the creation page.

3. In the **Select a template type** area, select **Blank Template**.

Note:

A policy template is used to create a policy by copying an existing policy (a preset or custom policy) and then modifying the policy. You can select an appropriate policy template to reduce the difficulty and workload of policy definition.

4. Click **Next** and rename the policy as needed (You can also retain the current policy name).

5. Copy and paste the following content in the **Policy Content** box:



```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "name/im:*"
      ],
      "resource": [
        "qcs::im::uin/12345678:sdkappid/1400000001",
        "qcs::im::uin/12345678:sdkappid/1400000002"
      ]
    }
  ]
}
```

```
    ]
  },
  {
    "effect": "deny",
    "action": [
      "name/im:RemoveUser"
    ],
    "resource": [
      "qcs::im::uin/12345678:sdkappid/1400000001"
    ]
  }
]
```

Note:

The policy content must comply with the CAM policy syntax logic described in [Element Reference](#). For more information on the syntax for resource and action elements, see [Resource syntax description](#) and [Action syntax description](#).

6. Click Done.

The method for granting the policy to other sub-accounts is the same as [Granting IM Permissions to an Existing Sub-account](#).

Using server APIs provided by CAM

For most developers, performing permission management operations in the console can meet their business needs. However, if you need to automate and systematize your permission management capabilities, you can use server APIs.

Policy-related server APIs are included in CAM. For more information, see [CAM documentation](#). Among these APIs, the major ones include:

[CreatePolicy](#)

[DeletePolicy](#)

[AttachUserPolicy](#)

[DetachUserPolicy](#)