

# Customer Identity Access Management Operation Guide



#### Copyright Notice

©2013–2023 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

## Operation Guide

### Configuration Guide Steps

### User Management Directory

- Creating a user pool

- Switching user pools

- Setting the default user pool

- Editing a user pool

- Deleting a user pool

### User management

- Creating a user

- Viewing user details

- Editing user attributes

- Deleting a user

- Reset Password

- Freezing or locking users

- User group management

- Custom attributes

  - Creating a custom attribute

  - Editing a custom attribute

  - Viewing custom attributes

  - Deleting a custom attribute

### Application Management

- Creating an application

- App Configuration

- Experience the Application

### Authentication management

- General authentication sources

  - Creating an authentication source

    - Account and Password Authentication

    - SMS OTP

    - Email OTP

  - Editing an authentication source

    - Account and Password Authentication

    - SMS OTP

    - Email OTP

  - Testing an authentication source

  - Disabling or deleting an authentication source

### SNS authentication source

  - Creating an authentication source

    - PC WeChat Login

    - WeChat webpage login

    - WeChat Mini Program login

    - QQ login

    - Alipay Login

  - Editing an authentication source

  - Disabling or deleting an authentication source

### Audit Management

### Custom Settings

- Template Configuration

  - SMS templates

  - Email templates

Identity verification template  
Image CAPTCHA

## Operation Guide Configuration Guide Steps

Last updated: 2023-09-04 10:29:39

The configuration of the Customer Identity and Access Management (CIAM) console begins with the creation of a user directory. Once this is completed, operations such as enabling custom attributes, configuring authentication sources, and setting up applications can be initiated.

CIAM supports the configuration of multiple user directories, with all user data, custom attribute data, application data, and authentication source data isolated by user directory. Only after the administrator has completed the configuration of custom attributes and authentication sources can the application configuration be finalized. It is recommended to follow the steps below for configuration:

### **Step One: Establishing a User Directory**

The user directory serves as a prerequisite for user management, authentication, and login/registration services.

### **Step Two: Defining User Attributes**

The configuration of user attributes determines the user data maintained in the user directory.

### **Step Three: Creating an Authentication Source**

The platform supports social media authentication sources such as WeChat and QQ, enterprise authentication sources like LDAP/AD, and general authentication sources such as SMS and email.

### **Step Four: Creating an Application**

Customize general services such as login, registration, and password recovery for your application. The platform supports web applications, mobile apps, mini programs, and more.

### **Step Five: Experience the Configuration**

The platform provides a default configuration for beginner's demo applications and SDKs, allowing users to preview the effects in advance.

# User Management Directory

## Creating a user pool

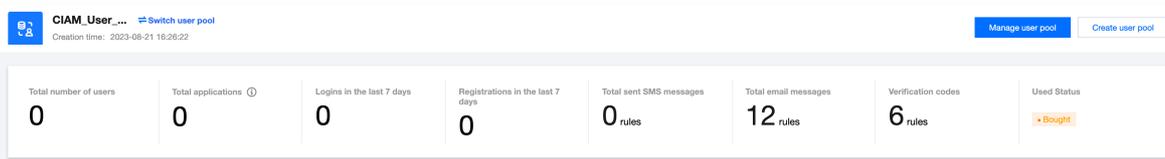
Last updated: 2023-09-04 10:29:49

### Scenario

The user pool serves as the primary directory in the Account Risk Control platform, isolating all user data, custom attribute data, application data, and authentication source data. Before using the Account Risk Control platform for the first time, you need to create a user pool. The platform supports the configuration of multiple user pools.

### Instructions

1. Log in to the [Account Risk Control Platform Console](#), select **Overview** from the left sidebar to navigate to the Overview page.
2. If this is your first time logging into the Account Risk Control Platform Console and you have not created a user pool before, you can click **Create Now** to experience the one-click creation feature. This feature automatically creates demo data, including applications, authentication sources, and other information.
3. On the Overview page, click **Create User Pool** in the upper right corner of the interface to open the Create User Pool pop-up window.



4. In the new user pool pop-up window, fill in the relevant information and click **OK** to complete the creation of the new user pool.

The screenshot shows the 'Create user pool' pop-up window. It has a title bar with 'Create user pool' and a close button. The form contains the following fields and elements:

- User pool name \***: A text input field with the placeholder text 'Enter the name'.
- Logo image**: A section with a circular icon containing a person and a plus sign, and the text 'You have not selecte...'. Below it is a 'Select an image' button.
- Upload a PNG or JPG file within 1 MB.**: A text instruction below the logo image section.
- OK** and **Cancel** buttons: Two buttons at the bottom of the form.

#### Parameter Description:

- **User Pool Name:** The name must be unique and non-empty, and cannot exceed 128 characters.
- **Logo Image:** Accepts .png or .jpg files smaller than 1 MB.

# Switching user pools

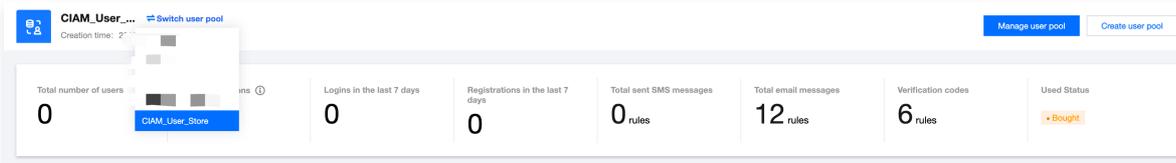
Last updated: 2023-09-04 10:29:56

## Scenario

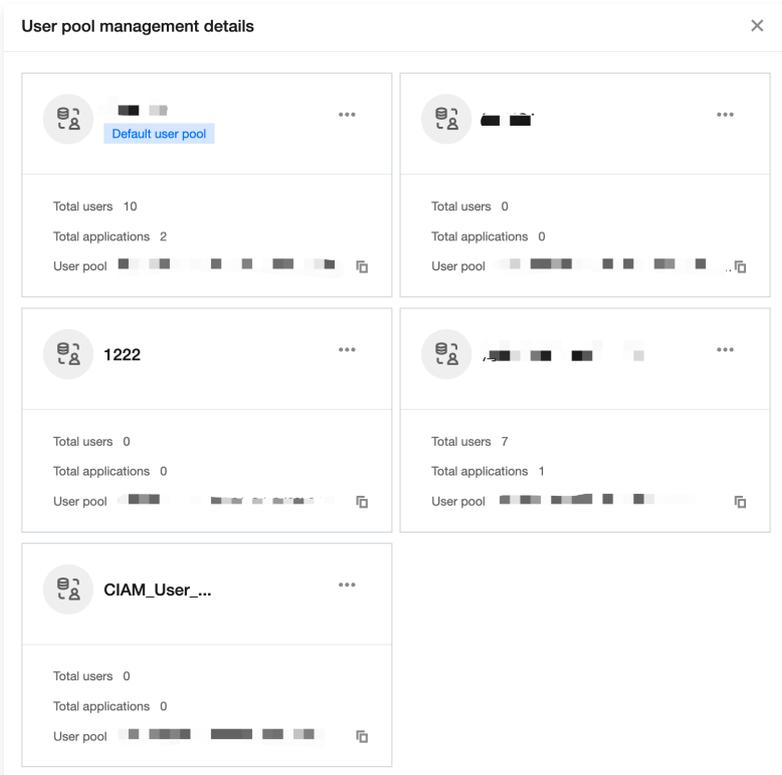
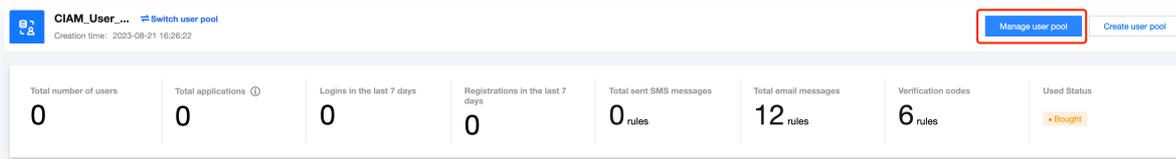
The Account Risk Control Platform supports multiple user directories. If an administrator needs to manage and configure different user directories, this can be accomplished by switching between user directories.

## Instructions

1. Log in to the [Account Risk Control Platform Console](#), select **Overview** from the left sidebar to navigate to the Overview page.
2. On the Overview page, directories can be switched in the following two ways:
  - Method 1: Click on **Switch User Directory** at the top left of the interface and select the directory you wish to switch to.



- Method 2: Click on **Manage User Directory** at the top right of the interface to enter the User Directory Management Details page, then select the directory you wish to switch to.



# Setting the default user pool

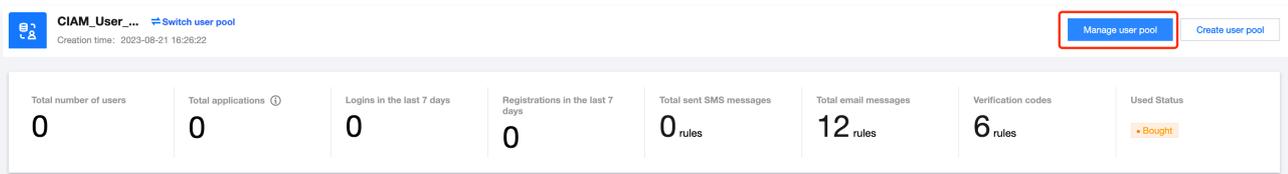
Last updated: 2023-09-04 10:31:50

## Scenario

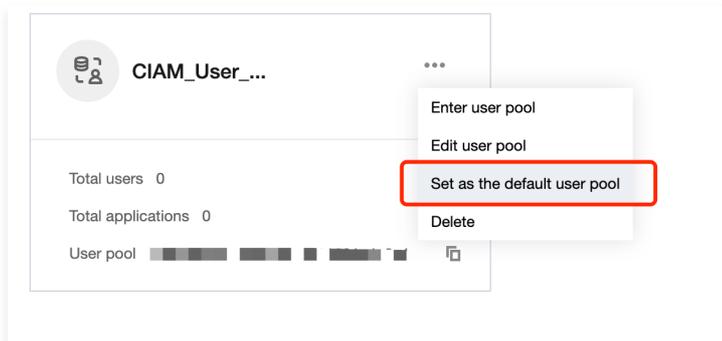
The Account Risk Control Platform supports multiple user directories. If an administrator has a user directory that needs to be managed as a priority, this can be accomplished by setting a default user directory. Once set, the administrator will automatically enter the designated user directory upon each login.

## Instructions

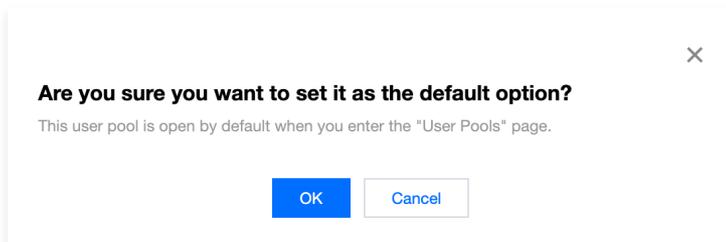
1. Log in to the [Account Risk Control Platform Console](#), select **Overview** from the left sidebar to navigate to the Overview page.
2. On the Overview page, click on **Manage User Directory** at the top right of the interface to enter the User Directory Management Details page.



3. On the User Directory Management Details page, click **...**, then select **Set as Default User Directory**.



4. In the "Confirm Settings" pop-up window, click **OK** to complete the setting of the default user directory.



# Editing a user pool

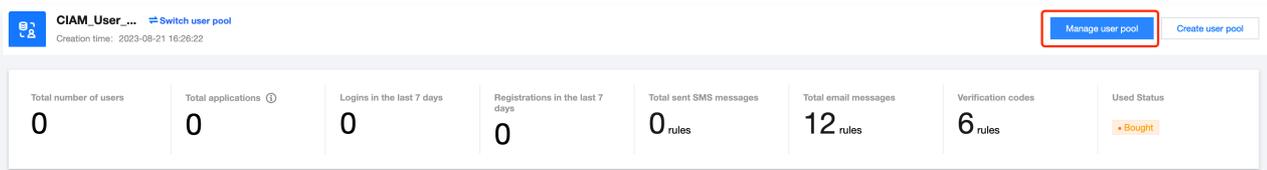
Last updated: 2023-09-04 10:31:57

## Scenario

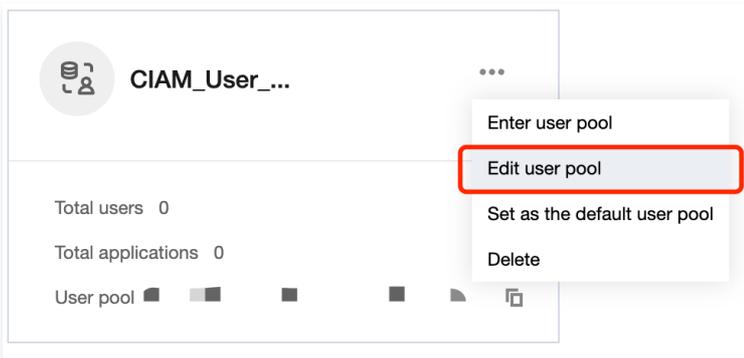
Upon successful creation of the user directory, you can modify the user directory information, such as the user directory name, Logo image, and so on.

## Instructions

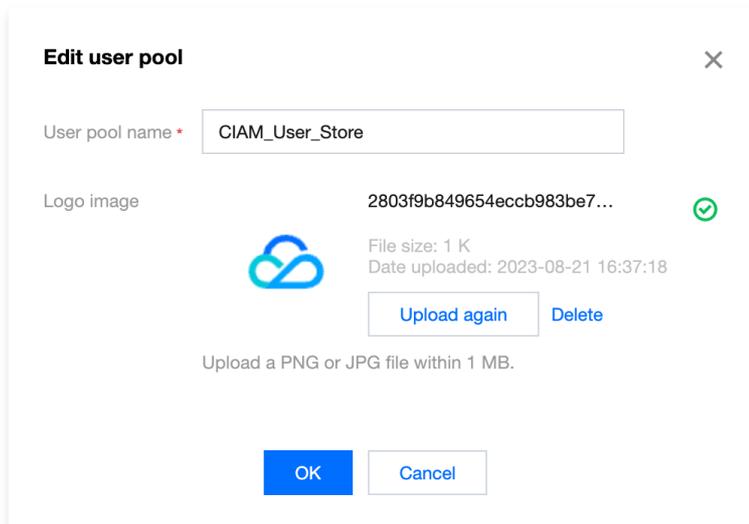
1. Log in to the [Account Risk Control Platform Console](#), select **Overview** from the left sidebar to navigate to the Overview page.
2. On the Overview page, click on **Manage User Directory** at the top right of the interface to enter the User Directory Management Details page.



3. On the User Directory Management Details page, click **...** and then click on **Edit User Directory**.



4. In the Edit User Directory pop-up window, after modifying the user directory information, click **Confirm**.



### Parameter Description:

- **User Pool Name:** The name must be unique and non-empty, and cannot exceed 128 characters.
- **Logo Image:** Accepts .png or .jpg files smaller than 1 MB.

# Deleting a user pool

Last updated: 2023-09-04 10:32:03

## Scenario

The Account Risk Control Platform supports multiple user directories. If an administrator no longer requires one or more of these directories, they can be removed by deleting the user directory.

### Note

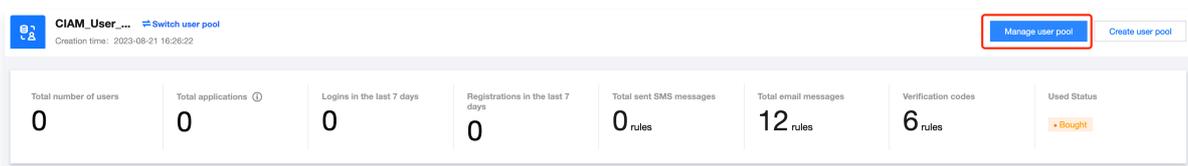
Deleting a user directory will erase all data within it, including users, custom attributes, user groups, applications, authentication sources, and all other information. Please proceed with caution.

## Preparations

Before deleting a user directory, any active applications must be closed.

## Instructions

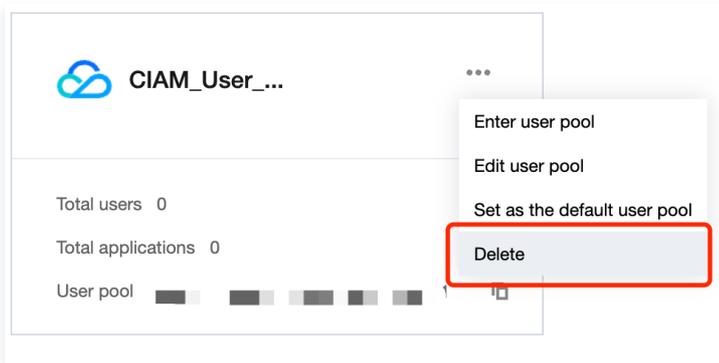
1. Log in to the [Account Risk Control Platform Console](#), select **Overview** from the left sidebar to navigate to the Overview page.
2. On the Overview page, click on **Manage User Directory** at the top right of the interface to enter the User Directory Management Details page.



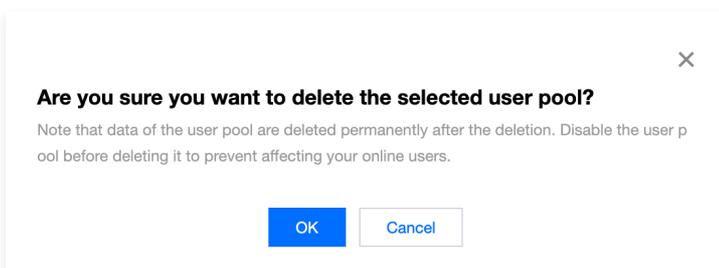
3. On the User Directory Management Details page, click **...**, then select **Delete**.

### Note

If operation protection has been enabled on the [Security Settings page](#) in the Account Center, a second verification of identity will be required when deleting a user directory. Within half an hour of passing the second verification, subsequent deletions will not require another round of verification.



4. In the "Confirm Deletion" pop-up window, click **OK** to complete the deletion of the user directory.



## User management

### Creating a user

Last updated: 2023-09-04 10:32:10

## Scenario

Upon successful creation of the user directory and custom attributes, you can proceed with the creation of new users.

## Instructions

1. Log in to the [Account Risk Control Platform](#), and select **User Management** > **User Management** from the left sidebar.
2. On the User Management page, click **Create User** to open the Create User dialog box.
3. In the Create User dialog box, after filling in the basic user information, click **OK** to successfully add the user.

### Note

The default status for a newly created user is disabled. Upon the user's first login, the status will change to normal.

### Create user

×  

|            |  |
|------------|--|
| 用户名称 *     | <input type="text" value="Please enter用户名称"/>  |
| Password * | <input type="password" value="Enter the password"/>  |
| 用户昵称       | <input type="text" value="Please enter用户昵称"/>  |
| 邮箱地址 *     | <input type="text" value="Please enter邮箱地址"/>  |
| Phone n... | <input type="text" value="+86"/> <input type="text" value="Please enter your phone number"/>   |
| 用户组        | <input type="text" value="Please enter用户组"/>   |
| 生日         | <input type="text" value="Please enter生日"/>        |
| 地址         | <input type="text" value="Please enter地址"/>  |

# Viewing user details

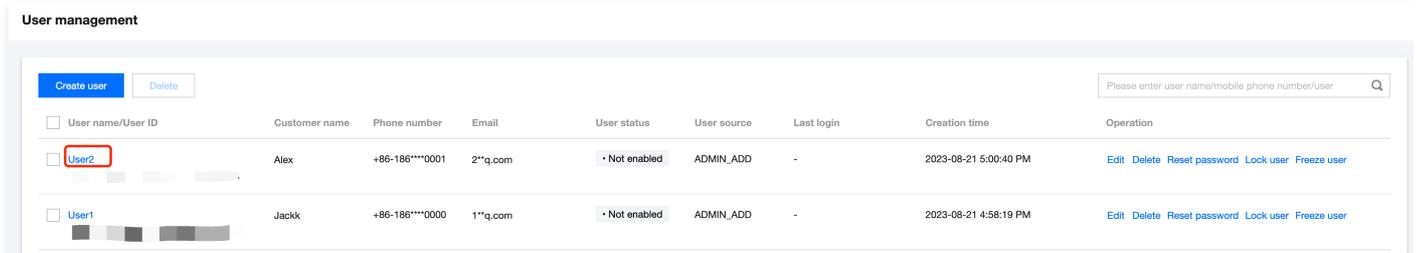
Last updated: 2023-09-04 10:32:16

## Scenario

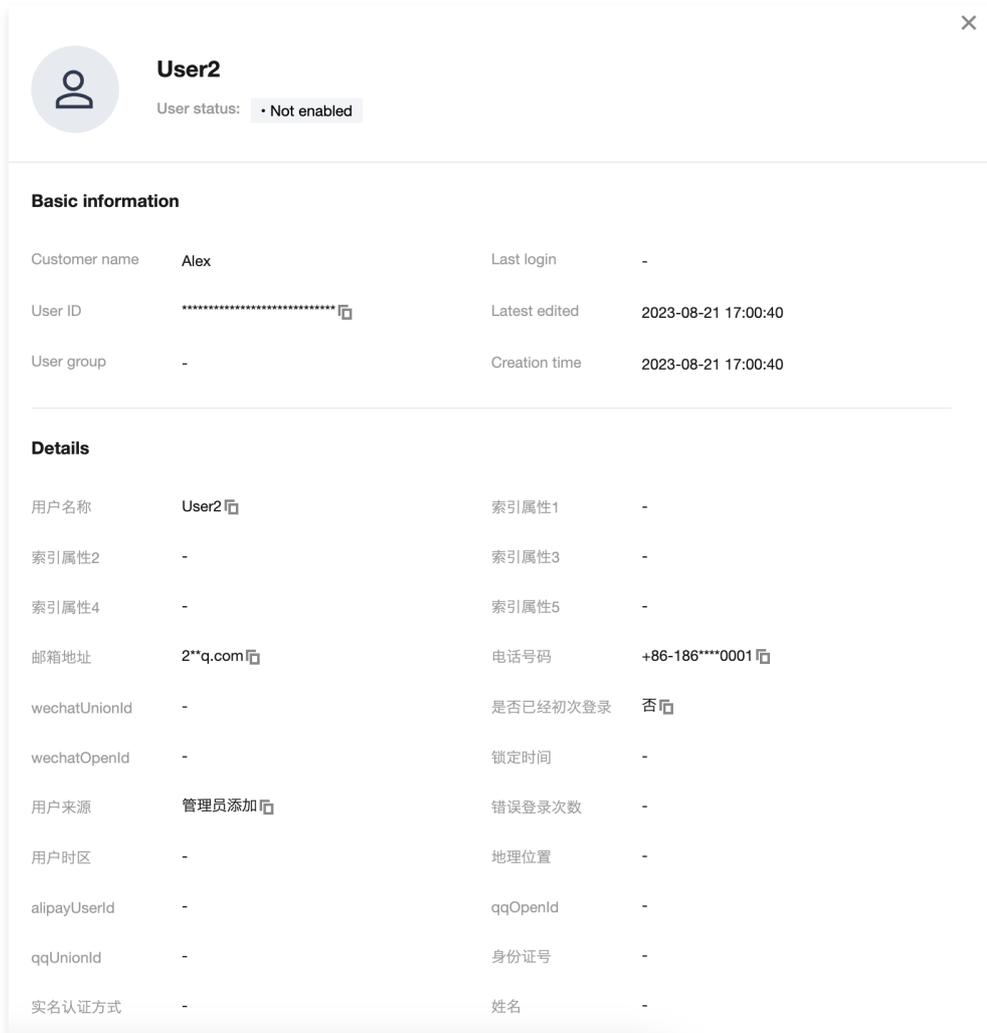
Upon successful addition of a user, you can view detailed user information, such as basic details and affiliated user groups.

## Instructions

1. Log in to the [Account Risk Control Console](#), and from the left navigation bar, select **User Management > User Management**.
2. On the User Management page, click on the "Username" to access the User Profile page.



3. On the User Profile page, you can view user information and the affiliated user groups.



# Editing user attributes

Last updated: 2023-09-04 10:32:21

## Scenario

Upon successful addition of a user, it is possible to modify user attribute information such as the user name, associated email, and phone number.

## Instructions

1. Log in to the [Account Risk Control Console](#), and from the left navigation bar, select **User Management > User Management**.
2. On the User Management page, click **Edit User** in the operation column to open the Edit User dialog box.

User management

Create user Delete

| <input type="checkbox"/> User name/User ID | Customer name | Phone number    | Email    | User status | User source | Last login | Creation time         | Operation   |
|--|---------------|-----------------|----------|-------------|-------------|------------|-----------------------|---|
| <input type="checkbox"/> User2             | Alex          | +86-186****0001 | 2**q.com | Not enabled | ADMIN_ADD   | -          | 2023-08-21 5:00:40 PM | <span>Edit</span> <span>Delete</span> <span>Reset password</span> <span>Lock user</span> <span>Freeze user</span> |
| <input type="checkbox"/> User1             | Jackk         | +86-186****0000 | 1**q.com | Not enabled | ADMIN_ADD   | -          | 2023-08-21 4:58:19 PM | <span>Edit</span> <span>Delete</span> <span>Reset password</span> <span>Lock user</span> <span>Freeze user</span> |

3. In the Edit User dialog box, after modifying the user information, click **OK**.

### Edit user

×  

用户名称

用户昵称

邮箱地址

Phone n...

用户组

生日

地址

OK Cancel

# Deleting a user

Last updated: 2023-09-04 10:32:27

## Scenario

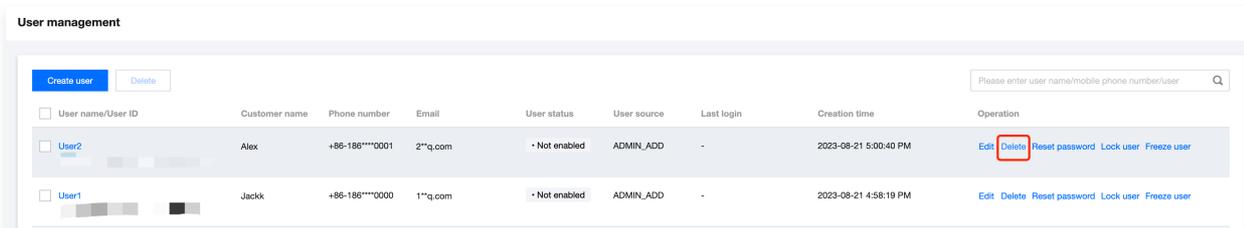
Upon successful addition of users, you have the option to delete individual or multiple users as per your requirements.

### Note

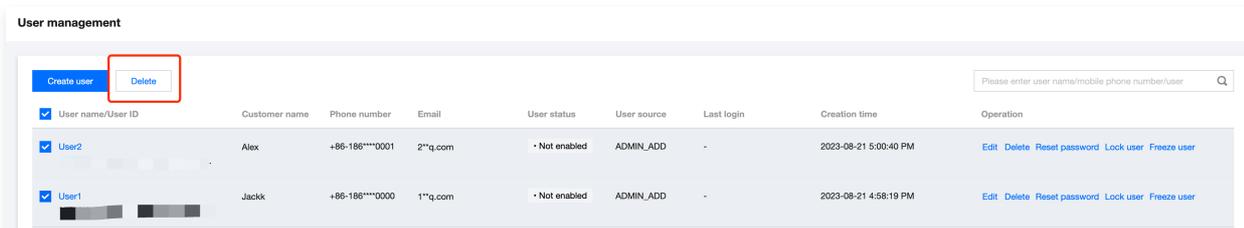
Note that after the deletion, all data will be cleared and cannot be restored.

## Instructions

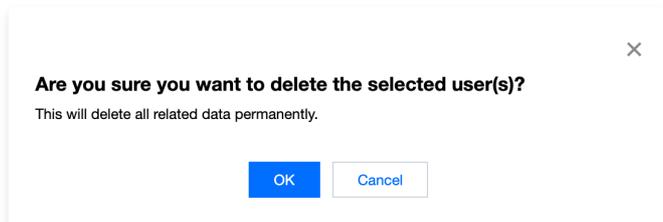
1. Log in to the [Account Risk Control Console](#), and from the left navigation bar, select **User Management > User Management**.
2. On the User Management page, you have the option to delete individual or multiple users.
  - To delete a single user: Select the user you wish to remove, then click on **Delete** in the "Actions" column. A confirmation pop-up will appear.



- To delete multiple users: Select one or more users that you wish to remove, then click **Delete** at the top of the list. A confirmation window will appear.



3. In the "Confirm Deletion" pop-up window, click **Confirm** to delete the selected users.



# Reset Password

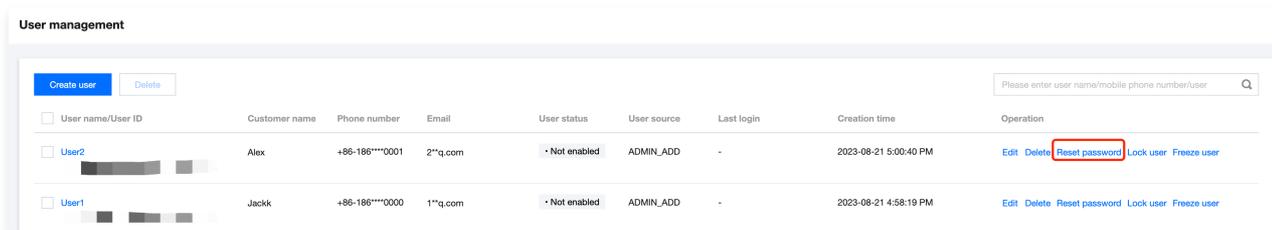
Last updated: 2023-09-04 11:19:40

## Scenario

In the event that a user forgets their login password, or their account is locked due to a certain number of failed login attempts, they can reset their password.

## Instructions

1. Log in to the [Account Risk Control Console](#), and from the left navigation bar, select **User Management > User Management**.
2. On the User Management page, click **Reset Password** in the "Operation" column. A "Confirm Password Reset" pop-up window will appear.



The screenshot shows the 'User management' interface. At the top, there are 'Create user' and 'Delete' buttons, and a search bar with the placeholder text 'Please enter user name/mobile phone number/user'. Below is a table with columns: 'User name/User ID', 'Customer name', 'Phone number', 'Email', 'User status', 'User source', 'Last login', 'Creation time', and 'Operation'. Two users are listed: 'User2' (Alex, +86-186\*\*\*\*0001, 2@qq.com, Not enabled, ADMIN\_ADD, -, 2023-08-21 5:00:40 PM) and 'User1' (Jackk, +86-186\*\*\*\*0000, 1@qq.com, Not enabled, ADMIN\_ADD, -, 2023-08-21 4:58:19 PM). In the 'Operation' column for 'User2', the 'Reset password' button is highlighted with a red box.

| User name/User ID | Customer name | Phone number    | Email    | User status | User source | Last login | Creation time         | Operation   |
|-------------------|---------------|-----------------|----------|-------------|-------------|------------|-----------------------|---|
| User2             | Alex          | +86-186****0001 | 2@qq.com | Not enabled | ADMIN_ADD   | -          | 2023-08-21 5:00:40 PM | Edit Delete <b>Reset password</b> Lock user Freeze user |
| User1             | Jackk         | +86-186****0000 | 1@qq.com | Not enabled | ADMIN_ADD   | -          | 2023-08-21 4:58:19 PM | Edit Delete Reset password Lock user Freeze user        |

3. In the "Confirm Password Reset" pop-up window, click **Confirm** to reset the password.

### Note

Resetting the password will unlock the account.

### Are you sure you want to reset the password?

This account will be unlocked after the password is reset

OK Cancel

# Freezing or locking users

Last updated: 2023-09-04 10:32:39

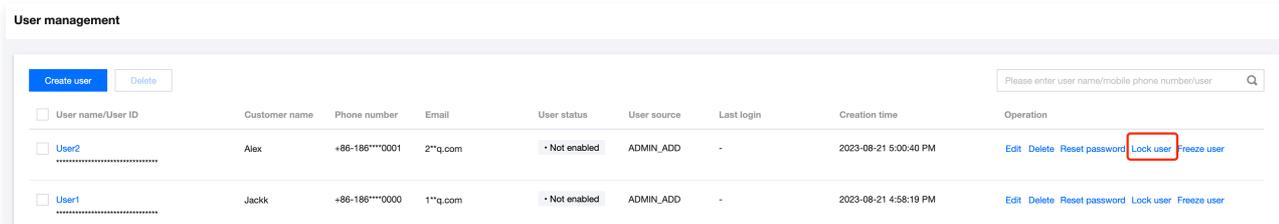
## Scenario

Upon successful addition of a user, you have the option to lock or freeze the user, preventing them from logging into the Risk Control Platform console.

## Instructions

### Locking a User

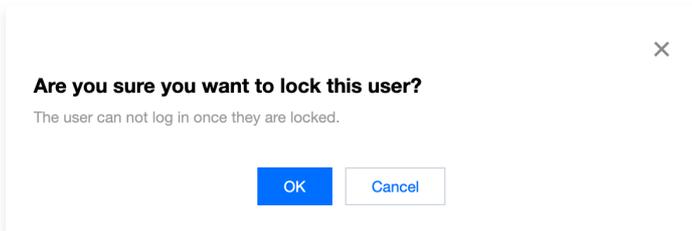
1. Log in to the [Account Risk Control Console](#), and from the left navigation bar, select **User Management > User Management**.
2. On the User Management page, click **Lock User** in the operation column. A "Confirm Lock" pop-up window will appear.



3. In the "Confirm Lock" pop-up window, click **OK**. The user will then be locked and unable to log in to the console.

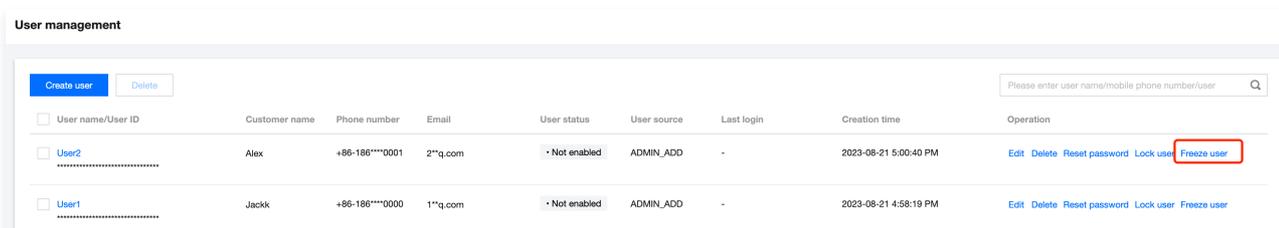
#### Note

- If the lock was initiated by an admin, it must be unlocked by an admin.
- If a user login triggers the lock policy, the unlock policy within the lock policy will automatically initiate the unlocking process.



### Freeze user

1. Log in to the [Account Risk Control Console](#), and from the left navigation bar, select **User Management > User Management**.
2. On the User Management page, click **Freeze User** in the operation column. A "Confirm Freeze" pop-up window will appear.



3. In the "Confirm Freeze" pop-up window, click **OK**. The user will then be frozen and unable to log into the console.

✕

**Are you sure you want to freeze the current user?**

After freezing, any logins of the user will be blocked

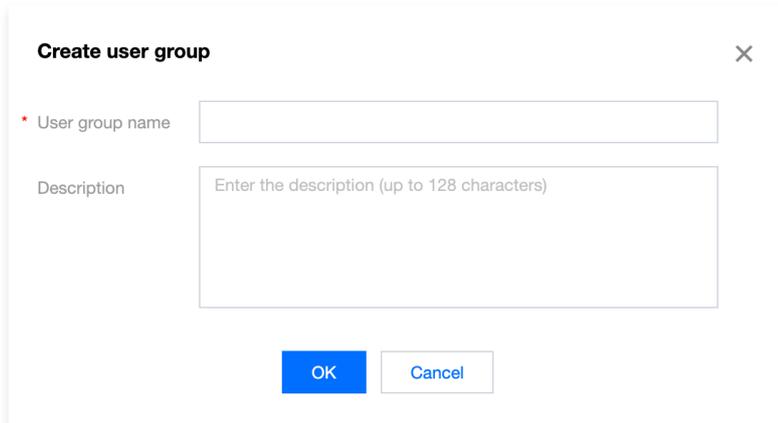
# User group management

Last updated: 2023-09-04 11:21:24

This document outlines the process of adding and editing user groups in the Account Risk Control console, as well as adding or removing users within these groups.

## Create user group

1. Log in to the [Account Risk Control console](#) and click on **User Group Management** in the left sidebar.
2. On the User Group Management page, click **Create User Group**.
3. In the Create User Group pop-up window, enter the user group name and notes, then click **OK** to complete the creation of the user group.



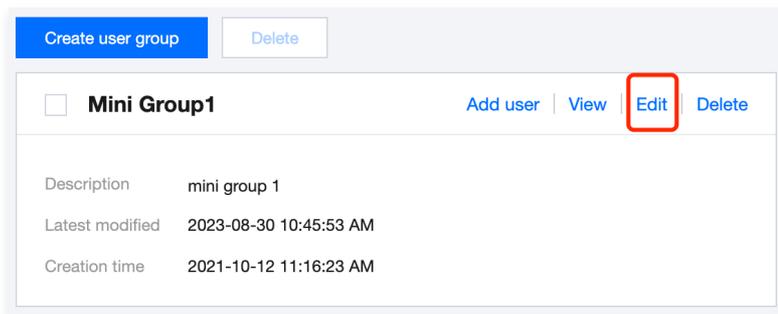
### Parameter Description:

- User Group Name: A custom name that must be unique.
- Note: Enter a custom description, not exceeding 128 characters.

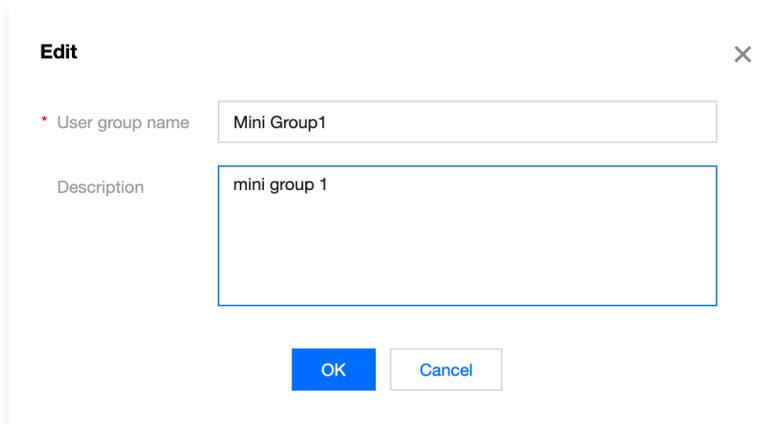
## Edit User Group

After creating a new user group, you have the ability to modify the user group name and notes.

1. On the [User Group Management](#) page, select the desired user group and click **Edit** below the user group.



2. In the edit pop-up window, modify the user group name and notes, then click **OK** to confirm.



**Edit** [Close]

\* User group name: Mini Group1

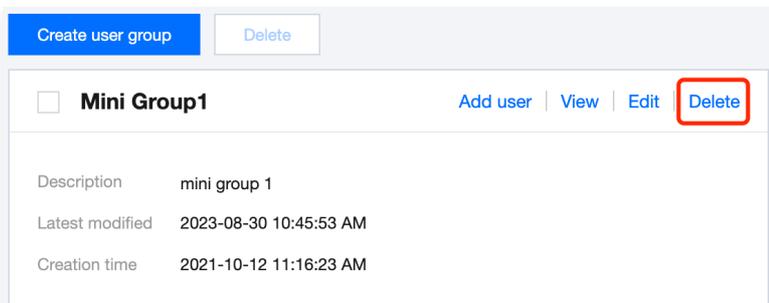
Description: mini group 1

[OK] [Cancel]

## Delete user group

After adding a new user group, if the added group is no longer needed, you can delete individual user groups or batch delete user groups on the [User Group Management page](#).

- Method 1: Select the desired user group and click **Delete** below the user group. After a second confirmation, the user group can be deleted.



[Create user group] [Delete]

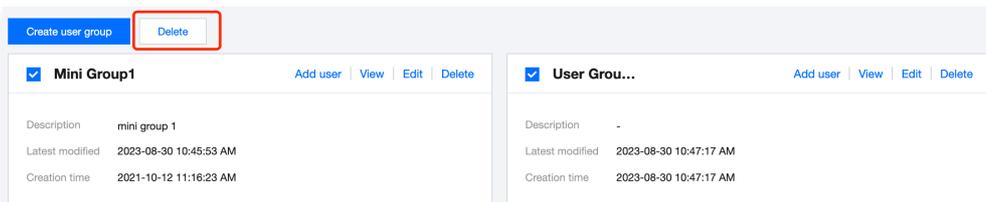
**Mini Group1** [Add user] [View] [Edit] [Delete]

Description: mini group 1

Latest modified: 2023-08-30 10:45:53 AM

Creation time: 2021-10-12 11:16:23 AM

- Method 2: Select one or more user groups that need to be deleted, click **Delete** above the user group list. After a second confirmation, the user group can be deleted.



[Create user group] [Delete]

**Mini Group1** [Add user] [View] [Edit] [Delete]

Description: mini group 1

Latest modified: 2023-08-30 10:45:53 AM

Creation time: 2021-10-12 11:16:23 AM

**User Grou...** [Add user] [View] [Edit] [Delete]

Description: -

Latest modified: 2023-08-30 10:47:17 AM

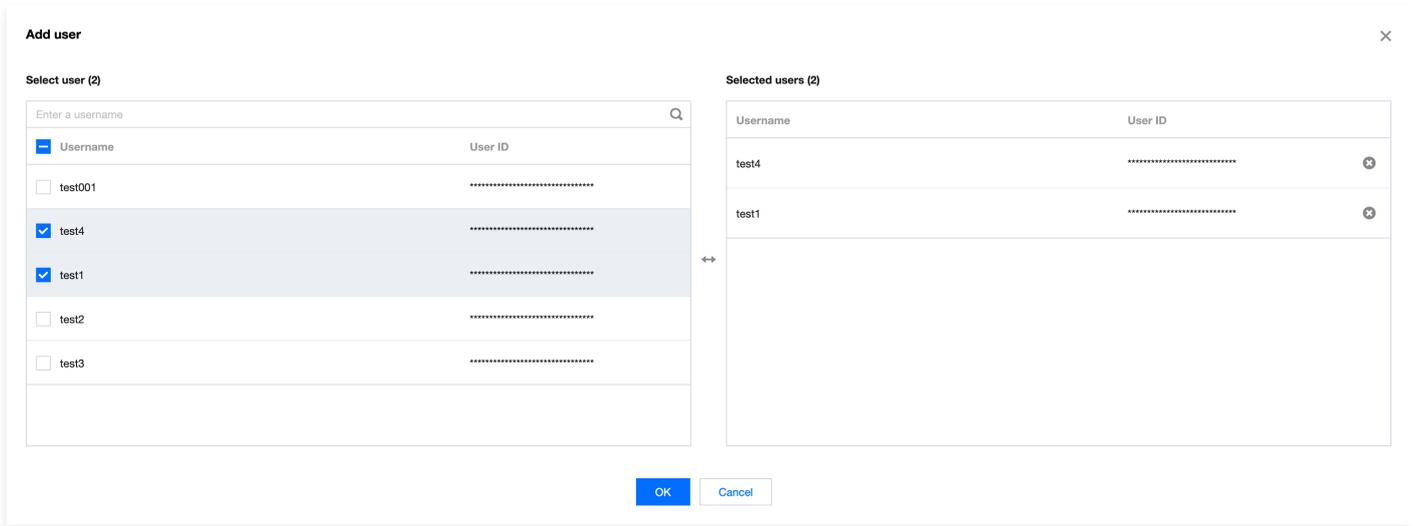
Creation time: 2023-08-30 10:47:17 AM

## Adding users to the user group

After creating a new user group, users can be added to this group.

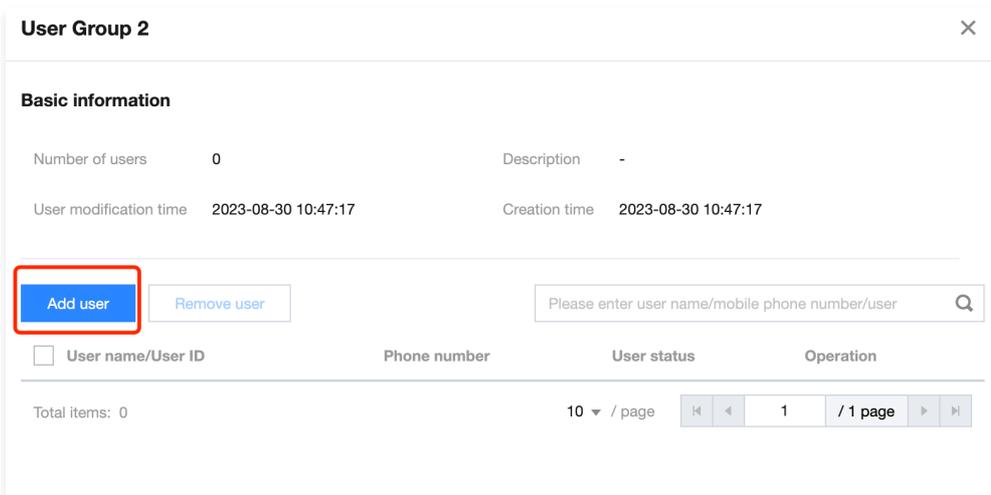
### Method 1

1. On the [User Group Management](#) page, select the desired user group and click **Add User** below the user group.
2. In the Add User pop-up window, select the users you wish to add and click **OK**. The selected users will be added to the user group.

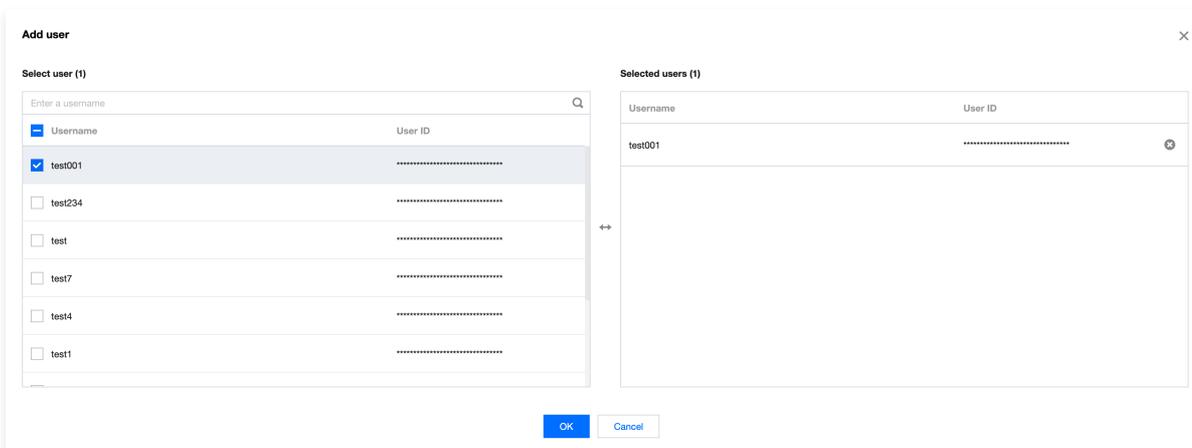


### Method 2

1. On the [User Group Management](#) page, select the desired user group and click on its blank area to enter the User Group Details page.
2. On the User Group Details page, click **Add User**.



3. In the Add User pop-up window, select the users you wish to add and click **OK**. The selected users will be added to the user group.

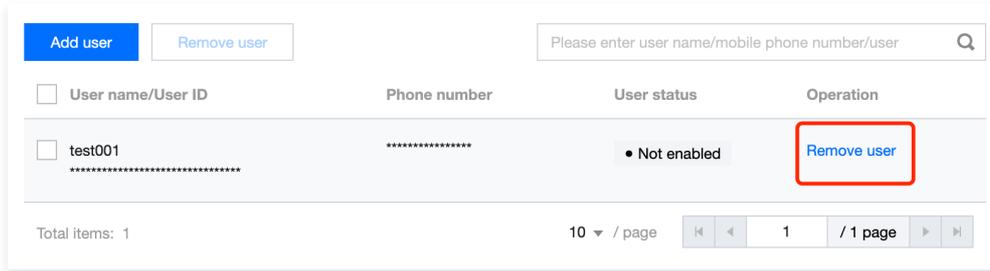


### Remove user from user group

After adding a user to a user group, you have the option to remove them.

**Method 1**

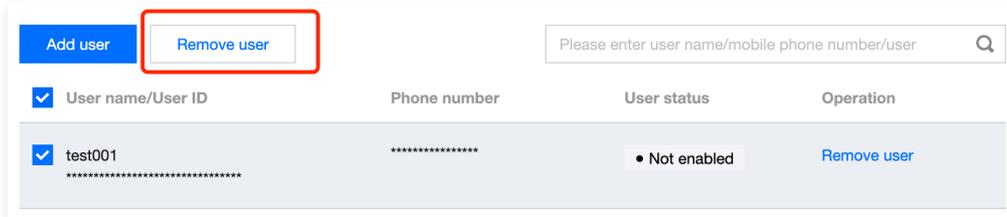
1. On the [User Group Management](#) page, select the desired user group and click on its blank area to enter the User Group Details page.
2. On the User Group Details page, click **Remove User** in the operation column on the right.



3. In the confirmation pop-up window, click **OK** to remove the user from the user group.

**Method 2**

1. On the [User Group Management](#) page, select the desired user group and click on its blank area to enter the User Group Details page.
2. On the User Group Details page, select one or more users to be removed and click **Remove User** at the top.



# Custom attributes

## Creating a custom attribute

Last updated: 2023-09-04 10:32:53

### Scenario

After successfully creating the [User Directory](#), you can proceed to create custom attributes.

#### Note

Custom attributes provide tenants with the functionality to define user attribute models, including built-in attributes, preset attributes, and custom attributes, with support for user-defined attributes. Built-in attributes cannot be modified or deleted, while preset and custom attributes can be modified and deleted. Once user data is generated, the associated preset and custom attributes cannot be modified, so please proceed with caution.

### Instructions

1. Log in to the [Account Risk Control Platform Console](#), and in the left sidebar, select **User Management > Custom Attributes**.
2. On the Custom Attributes page, click **Create Attribute**. A "Create Attribute" pop-up window appears.
3. In the 'Create Attribute' pop-up window, fill in the basic attribute information and click **OK** to successfully add it. If necessary, you can also add a regular expression and error message for the attribute.

#### Create attribute field ✕

\* Attribute name

\* Attribute label

\* Field Type

Data masking rules

**Regex** ▲

Regular Expression

Error

# Editing a custom attribute

Last updated: 2023-09-04 10:32:58

## Operational Overview

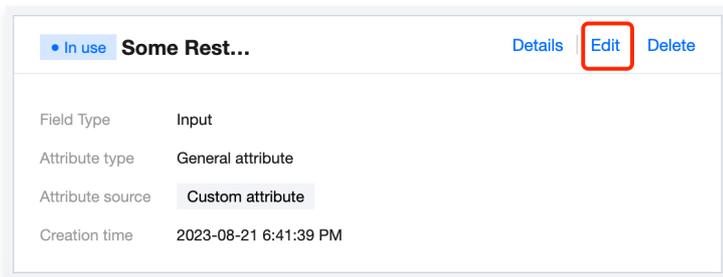
Upon successful addition of a custom attribute, you can modify information such as the attribute field, regular expressions, and error prompts.

### Note

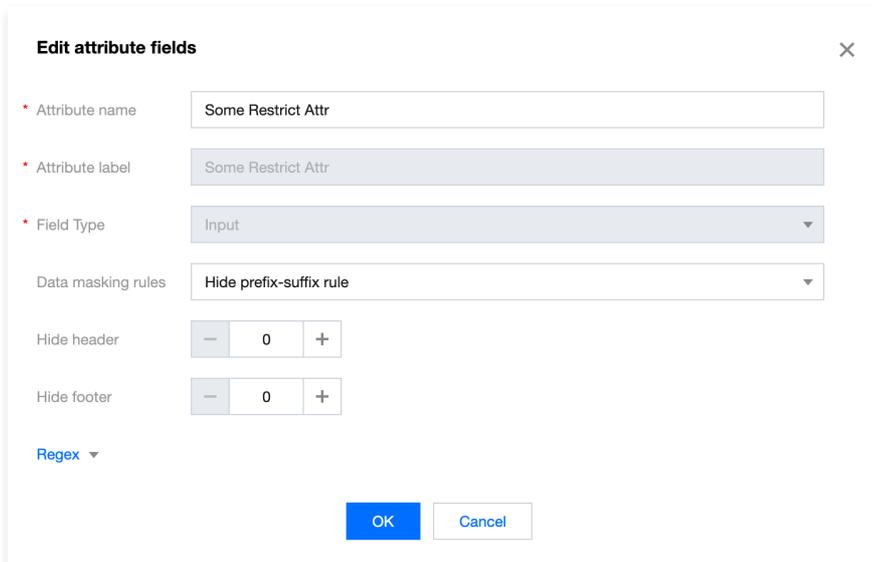
Inbuilt attributes cannot be edited, while preset and custom attributes are editable.

## Instructions

1. Log in to the [Account Risk Control Platform Console](#), and in the left sidebar, select **User Management > Custom Attributes**.
2. On the Custom Attributes page, click **...** > **Edit Details**.



3. In the Edit Properties pop-up window, after modifying the attribute information, click **Confirm**.



The screenshot shows the 'Edit attribute fields' pop-up window. It has a title bar with a close button (X). The form contains the following fields:

- Attribute name: Some Restrict Attr
- Attribute label: Some Restrict Attr
- Field Type: Input (dropdown menu)
- Data masking rules: Hide prefix-suffix rule (dropdown menu)
- Hide header: 0 (with minus and plus buttons)
- Hide footer: 0 (with minus and plus buttons)
- Regex: (dropdown menu)

At the bottom, there are 'OK' and 'Cancel' buttons.

# Viewing custom attributes

Last updated: 2023-09-04 10:33:02

## Scenario

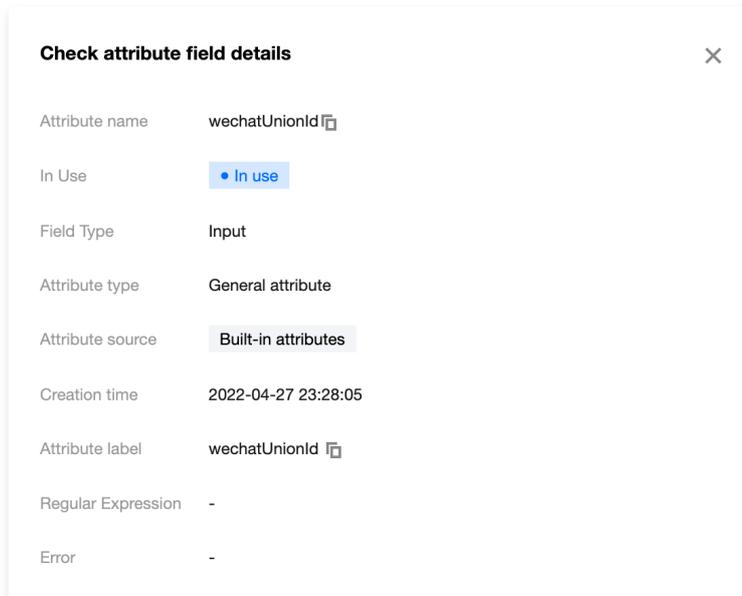
Upon successful addition of a custom attribute, one can view details such as attribute fields, regular expressions, and error prompts.

## Instructions

1. Log in to the [Account Risk Control Platform Console](#), and in the left sidebar, select **User Management > Custom Attributes**.
2. On the  page, click **> View Details**.



3. In the View Field Attributes pop-up window, you can view the details of the field attributes.



# Deleting a custom attribute

Last updated: 2023-09-04 10:33:09

## Scenario

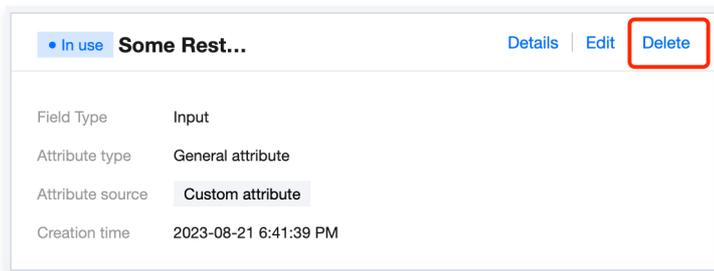
Upon successful addition of a custom attribute, it is possible to delete information related to the custom attribute, such as attribute fields, regular expressions, and error prompts.

### Note

Inbuilt attributes cannot be deleted, while preset and custom attributes are deletable.

## Instructions

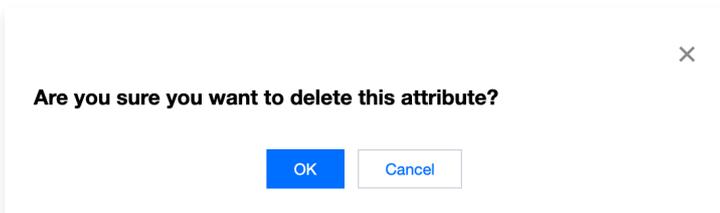
1. Log in to the [Account Risk Control Platform Console](#), and in the left sidebar, select **User Management > Custom Attributes**.
2. On the Custom Attributes page, click **...** > **Delete**.



3. In the confirmation pop-up window, click **OK** to delete the selected attribute.

### Note

Note that after the deletion, this custom attribute can not be recovered. Please disable the attribute first to prevent affecting your online users.



# Application Management

## Creating an application

Last updated: 2023-09-04 10:33:47

### Scenario

The Account Risk Control Platform allows administrators to create business applications for external use, supporting a variety of application types including Web applications, mobile apps, single-page applications, mini program applications, and M2M applications. Before configuring parameters, registration/login processes, and other procedures for the business application, administrators must first create the application.

### Instructions

1. Log in to the [Account Risk Control Platform console](#) and select **Application Management** from the left sidebar.
2. On the Application Management page, click **New Application** in the operation column to open the New Application dialog box.
3. In the New Application dialog box, fill in the required information as prompted, then click **Confirm** to create a new application.

#### Note

Fields marked with an asterisk (\*) are required.

### Create application

Application icon \*      application\_default.svg



Upload a PNG or JPG file within 1 MB.

Template Name \*     

Application type \*     

Industry     

Description     

One-page application

Mobile App

Web application

WeChat Mini Program application

M2M application

# App Configuration

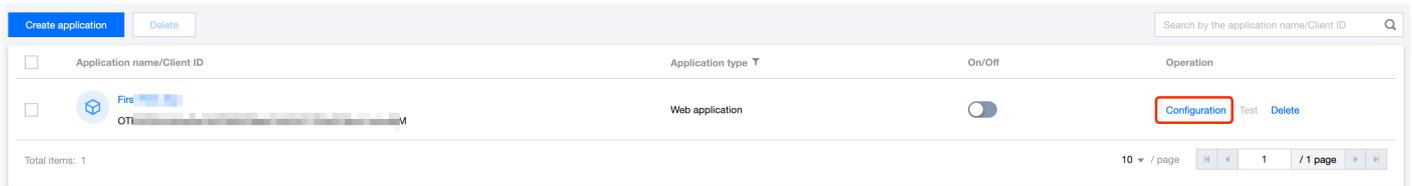
Last updated: 2023-09-04 11:28:24

## Scenario

The Account Risk Control Platform allows administrators to configure applications according to business requirements. This includes basic information configuration (such as icons and names), parameter configuration (such as redirect and logout addresses), and process configuration (such as registration, login, and password recovery).

## Instructions

1. Log in to the [Account Risk Control Platform console](#) and select **Application Management** from the left sidebar.
2. On the Application Management page, click **Configuration** in the operation column to access the basic information page for application configuration.



## Basic information

On the Basic Information page, you can modify the application icon, name, type, description, and industry. After making changes, click **Confirm** to save.

← **Application configuration**

**Basic information** | Parameter configuration | Process configuration | CORS

Application icon • application\_default.svg  
 [Select an image](#)  
[Delete](#)  
Upload a PNG or JPG file within 1 MB.

Template Name •

Application type • **Web application**

Industry

Client ID

Secret

Description

## Parameter configuration

1. On the Application Configuration page, click on **Parameter Settings** to switch to the parameter configuration page for the application.
2. On the Parameter Configuration page, fill in the required information and click **OK** to save.

**Application configuration**

Basic information **Parameter configuration** Process configuration CORS

Redirect URI [Add](#)

Enter the complete URI addresses starting with the protocol (for example https://example.com/callback). These URIs are used to receive the authentication code for OAuth protocol. Up to 10 URIs allowed.

Logout Redirect URI [Add](#)

Enter the complete URI address starting with the protocol (for example https://example.com/logout). These URIs are used as the direction addresses when the user logs out. Up to 10 URIs allowed.

Access\_token validity  seconds

refresh\_token  Enable refresh\_token

Claims

| Category                      | Description  | Sample value  |
|-------------------------------|--|---|
| Redirect URI                  | Enter a complete URL starting with http or https to receive the authorization code from the OAuth protocol. After the user grants permission, they will be redirected to this address with the code. | <a href="https://www.qq.com">https://www.qq.com</a>               |
| Logout Redirect URI           | Enter a complete URL starting with http or https, which will serve as the redirect address after the user logs out.  | <a href="https://www.qq.com/logout">https://www.qq.com/logout</a> |
| Access_token Validity Period  | The default validity period for the access_token is 600 seconds.   | 600   |
| refresh_toke                  | Is refresh token enabled?  | -   |
| Refresh_token Validity Period | The validity period of the refresh_token, specified when the token needs to be refreshed, is set to 86,400 seconds by default.   | 86400   |

### Process Configuration

Process configuration primarily includes the setup for registration, login, MFA, forgotten username, and forgotten password processes. By configuring different parameters, you can customize the application to meet various requirements for registration, login, and other processes.

For Web, single-page, and mobile App types of applications, configuration is supported for registration, login, MFA, forgotten username, and forgotten password processes. For mini-program applications, only registration/login process configuration is required.

#### Configuration for Web, Single Page, and Mobile App Applications

- On the Application Configuration page, click **Parameter Settings** to switch to the parameter configuration page for process configuration.
- The Parameter Configuration page includes five major modules: Registration Process, Login Process, MFA Process, Forgotten Username Process, and Forgotten Password Process.
  - Registration Process:** Click **Edit** in the upper right corner of the module, configure the relevant parameters, and click **OK** to save the configuration.

### Registration

- On/Off
- Authentication attribute Select the authentication attribute
- General attribute Add
- User group Select the user group
- Auto login
- Identity Verification
- Verification method ⓘ Two-factor verification ✔
- Registration result  Still register if verification fails  Do not register if verification fails
- Consent statement
- Content ⓘ 

Enter up to 1024 characters

 Required Add

OK
Cancel

**Parameter Description:**

- **Enabled:** By default, the feature is enabled. If disabled, users will not be able to register.
- **Authentication Attribute:** Required for user registration and can be used as a unique user identifier.
- **SMS OTP Authentication Source:** The strategy for sending SMS OTP during registration. This needs to be selected when the authentication attribute is set to phone number.
- **Email OTP Authentication Source:** This is the strategy for sending SMS OTP during registration. It needs to be selected when the authentication attribute is set to email address.
- **General Attributes:** Required for user registration but cannot be used as a unique user identifier.
- **User Group:** The group to which the user belongs after successful registration.
- **Auto Login:** Enable auto login so that users are automatically logged into the application after successful registration. Otherwise, they will be redirected to the login page for manual login.
- **Identity Verification:** Enable identity verification, you can choose two-factor or three-factor verification. The registration result can be set to either register despite verification failure or not register if verification fails.
- **Consent Statement:** Enabling the consent statement allows you to set the consent statement on the registration page. The setup instructions are as follows.

**Instructions**

Input format Text + Markdown hyperlink

Restrictions Up to 4 statements can be created and can be set as required or optional

Samples

| Statement input    | Details  | User-side display                      |
|--------------------|--|--|
| Markdown hyperlink | I agree to the [Privacy Policy] (https://www.qq.com) | I agree <a href="#">Privacy policy</a> |

- **Login Process:** Click **Edit** in the upper right corner of the module, configure the relevant parameters, and click **OK** to save the configuration.

**Login**

• On/Off

• Preferred authentication source

Associate authentication source

Remember password

Consent statement

**Parameter Description:**

- **Enabled Status:** Enabled by default. If disabled, users will not be able to log in.
- **Preferred Authentication Source:** The primary authentication method displayed on the login page.
- **Associated Authentication Source:** The alternative authentication methods displayed on the login page.
- **Claims:** The user attribute fields returned by the Get Token and Get User Information interfaces.
- **Remember Password:** Controls whether the browser remembers the password.
- **Consent Statement:** Enable the consent statement to set the consent statement on the login page.

**Instructions**

Input format Text + Markdown hyperlink

Restrictions Up to 4 statements can be created and can be set as required or optional

Samples

| Statement input    | Details  | User-side display                      |
|--------------------|--|--|
| Markdown hyperlink | I agree to the [Privacy Policy] (https://www.qq.com) | I agree <a href="#">Privacy policy</a> |

- **MFA Process:** Click **Edit** in the upper right corner of the module, configure the relevant parameters, and click **OK** to save the configuration.

**MFA process**

• On/Off

• Associate authentication source

**Parameter Description:**

- **Enable:** Not enabled by default. Once enabled, two-factor authentication will be activated.
- **Associate Authentication Source:** This includes two types of authentication methods, SMS OTP and Email OTP.
- **Process of Retrieving Username:** Click **Edit** in the upper right corner of the module, configure the relevant parameters, and click **OK** to save the configuration.

**Process of retrieving username**

\* On/Off

\* Retrieving method

---

**Parameter Description:**

- Enabled: By default, this feature is enabled. If disabled, users will not be able to retrieve their usernames.
- Recovery Method: The method for receiving the username, such as via email.
- **Reset Password Process:** Click **Edit** in the upper right corner of the module, configure the relevant parameters, and click **OK** to save the configuration.

**Process of resetting password**

\* On/Off

\* Retrieving method

\* Email OTP authentication source

---

**Parameter Description:**

- Enable: Enabled by default. If disabled, users will not be able to reset their passwords.
- Recovery Method: The method of receiving verification codes, used for resetting passwords, such as via email.
- Email OTP Source: The strategy for sending SMS OTP during registration. This needs to be selected when choosing email as the recovery method.

**Mini Program Application Configuration**

1. On the Application Configuration page, click **Parameter Settings** to switch to the parameter configuration page for process configuration.
2. On the Parameter Configuration page, you can configure the registration/login process. Click **Edit** in the upper right corner of the module, set the relevant parameters, and click **OK** to save the configuration.

**Registration/login**

\* On/Off

\* Preferred authentication source

---

**Parameter Description:**

- Enabled: By default, it is enabled. If disabled, users will not be able to register or log in.
- Preferred Authentication Source: Only Mini Program authentication sources can be selected.

**Security Domain CORS**

To call CIAM APIs using JavaScript, it is essential to configure a trusted CORS security domain. A maximum of 10 security domains can be configured.

1. On the Application Configuration page, click **Security Domain CORS** to switch to the security configuration page for the application.
2. On the Security Configuration page, click **Edit**.



3. After filling in the required information, click **Save** to confirm the configuration.



### Supports and Limits

- The application's Redirect URI has already been added to the CORS security domain by default, eliminating the need for redundant configuration here.
- The security domain should start with `https://` or `http://`, and the format should be `<protocol name> "://" <domain name or IP address> [ ":" <port number> ]`, for example, `https://sample.portal.tencentciam.com` or `http://127.0.0.1:8080`. It does not support carrying request paths.
- The domain section can only contain lowercase letters, numbers, periods (.), asterisks (\*), and hyphens (-). Within each segment of the domain, a hyphen cannot be used at the beginning or end, nor can there be consecutive hyphens. The first segment of the domain can be an asterisk (\*), representing a match for any subdomain, such as `https://*.example.com`. Asterisks are not permitted in other segments of the domain.

# Experience the Application

Last updated: 2023-09-04 10:34:01

## Scenario

Upon completion of the application configuration in the Account Risk Control Platform, you can swiftly experience the effects of the application configuration: operations such as application registration and login.

## Instructions

### Experience Web, Single Page, and Mobile App Applications

For Web applications, single-page applications, and mobile apps, you can quickly experience the effects of the configuration once the application is enabled.

1. Log in to the [Account Risk Control Platform Console](#), select **Application Management** in the left sidebar to enter the application management page.
2. On the Application Management page, click  of the application to be launched to start the application.

#### Note

During the application launch, a basic validation of the configuration information is performed. If the validation fails, modifications need to be made on the configuration page.

| <input type="checkbox"/> | Application name/Client ID   | Application type                | On/Off                              | Operation   |
|--------------------------|--|---------------------------------|-------------------------------------|---|
| <input type="checkbox"/> |  [redacted]  | Mobile App                      | <input checked="" type="checkbox"/> | <a href="#">Configuration</a> <a href="#">Delete</a>                      |
| <input type="checkbox"/> |  [redacted] | WeChat Mini Program application | <input type="checkbox"/>            | <a href="#">Configuration</a> <a href="#">Delete</a>                      |
| <input type="checkbox"/> |  [redacted] | Web application                 | <input type="checkbox"/>            | <a href="#">Configuration</a> <a href="#">Test</a> <a href="#">Delete</a> |

3. On the Application Management page, click **Experience** in the operation column to jump to the Demo demonstration page.

| <input type="checkbox"/> | Application name/Client ID   | Application type | On/Off                              | Operation   |
|--------------------------|--|------------------|-------------------------------------|---|
| <input type="checkbox"/> |  [redacted] | Web application  | <input checked="" type="checkbox"/> | <a href="#">Configuration</a> <a href="#">Test</a> <a href="#">Delete</a> |

4. On the Demo demonstration page, you can swiftly experience the application's registration, login, and other functions. After a successful login, you will be redirected to the following Demo page.

### 登录成功

前后端处理后续登录认证逻辑的最佳实践请参见本教程

|   |  |                    |
|---|--|--------------------|
|  | <b>处理回调</b><br>通过你的Web应用（有后端）或单页应用（无后端）处理回调。 | <a href="#">展开</a> |
|  | <b>获取用户信息</b><br>解析上一步返回的id_token，获取用户信息。    | <a href="#">展开</a> |
|  | <b>你可能还需要</b><br>阅读完本页面内容后，你可能还需要完成这些后续工作。   | <a href="#">展开</a> |

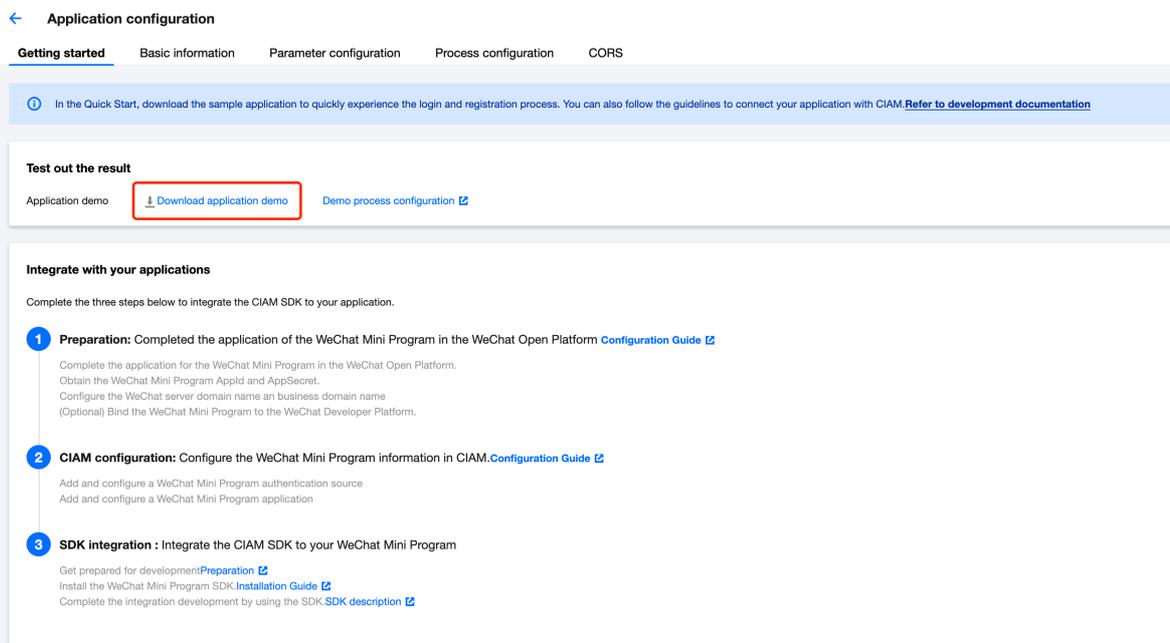
### Experience Mini Program Applications

For Mini Program application types, you need to integrate the SDK swiftly to complete the login and registration process effectively.

1. After creating a mini-program application, the administrator can go to the [Application Management Page](#), click **Configuration**, and enter the Quick Start page for application configuration.



2. On the Quick Start page, click **Download Sample Application**, and configure the SDK swiftly into your business application according to the [Sample Run Process Configuration](#).

A screenshot of the 'Application configuration' page in the Tencent Cloud console. The page has a breadcrumb trail: 'Application configuration' > 'Getting started' > 'Basic information' > 'Parameter configuration' > 'Process configuration' > 'CORS'. The 'Getting started' tab is selected. Below the breadcrumb, there is a blue information banner with a document icon and text: 'In the Quick Start, download the sample application to quickly experience the login and registration process. You can also follow the guidelines to connect your application with CIAM. Refer to development documentation'. Below this, there is a section titled 'Test out the result' with a sub-section 'Application demo' containing a 'Download application demo' button (highlighted with a red box) and a 'Demo process configuration' link. The main content area is titled 'Integrate with your applications' and contains three numbered steps: 1. Preparation, 2. CIAM configuration, and 3. SDK integration, each with detailed instructions and links to guides.

# Authentication management

## General authentication sources

### Creating an authentication source

#### Account and Password Authentication

Last updated: 2023-09-04 11:40:19

### Scenario

The Account Risk Control Platform supports the use of username–password authentication sources, which verifies user identities through the use of usernames and passwords.

### Instructions

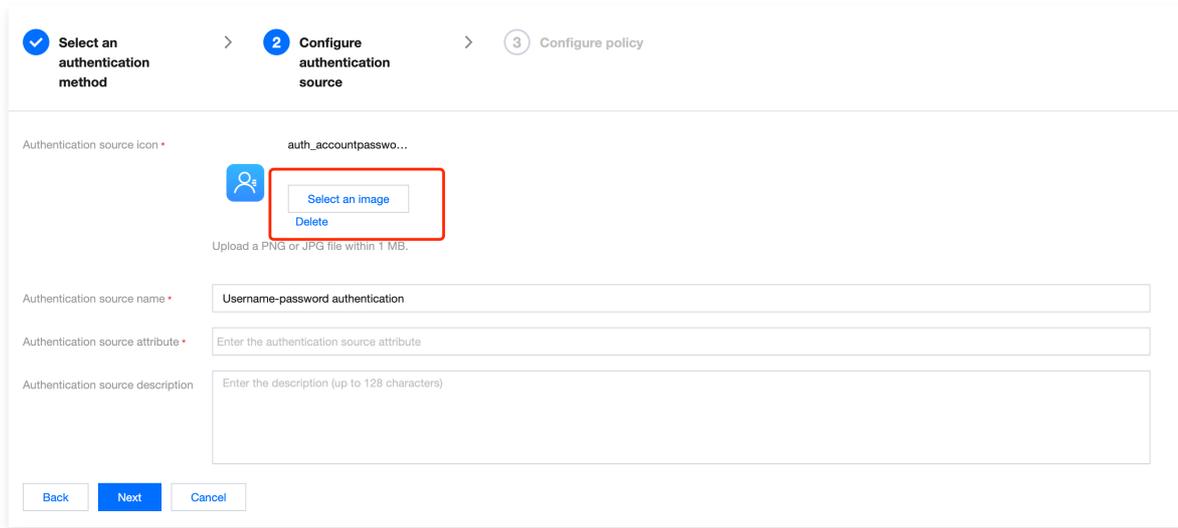
1. Log in to the [Account Risk Control Platform console](#), and select **Authentication Management > General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, click **Create Authentication Source** to navigate to the Create Authentication Source page.
3. On the Create Authentication Source page, select **Username–Password Authentication** and click **Next**.

The screenshot shows the 'Create Authentication Source' page. At the top, there is a progress bar with three steps: 1. Select an authentication method (active), 2. Configure authentication source, and 3. Configure policy. Below the progress bar, there are three options: 'Username-password authentication' (selected), 'Email OTP', and 'SMS OTP'. At the bottom, there are 'Next' and 'Cancel' buttons.

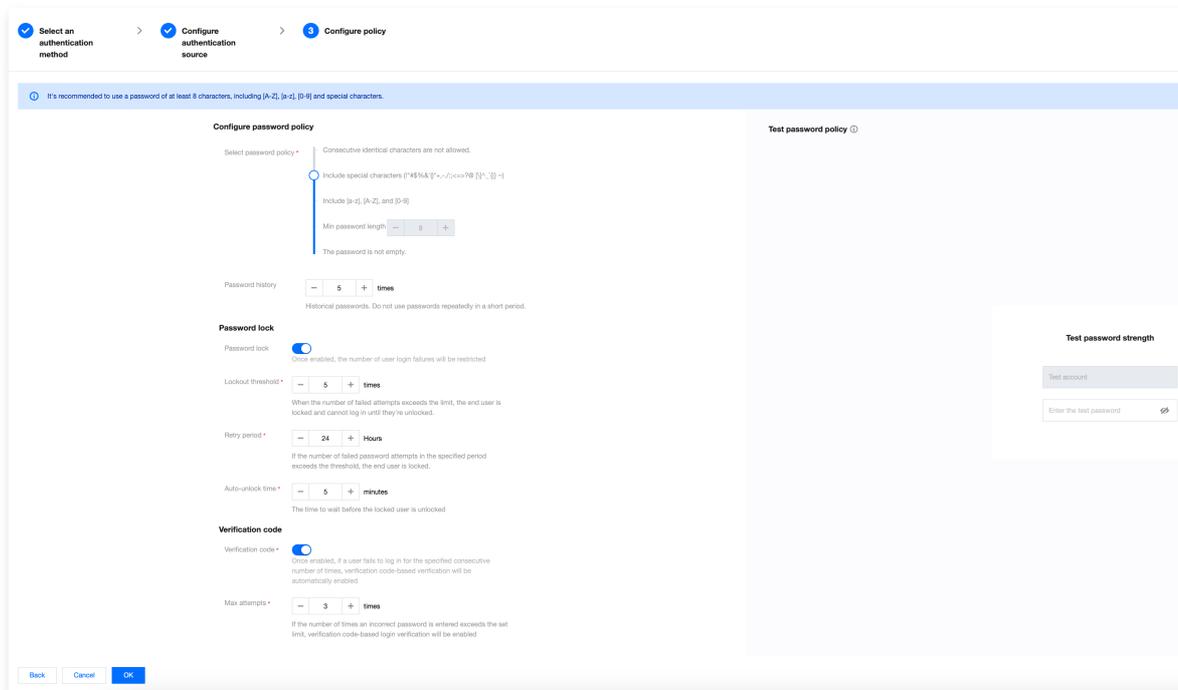
4. On the Create Authentication Source page, set the authentication source icon, name, attributes, and description, then click **Next**.

#### Note

- Authentication Source Icon: Displayed in the list and portal, users can click **Re-upload** to replace the default icon.
- Authentication Source Name: User Identity Authentication Source.
- Authentication Source Attributes: These are user attributes that can be used to confirm identity during username–password authentication.
- Authentication Source Description: A brief overview of the authentication source.



5. On the Create Authentication Source page, configure the relevant parameters and click **OK** to create the authentication source.



### Configure Policy Parameter Notes

- **Configure Password Policy**

- **Select Password Policy:** This is used to limit the strength of the passwords users can set. It supports five types of password policies, with the default policy being relatively strong.
- **Number of Historical Password Records:** To prevent the reuse of the same password within a certain period, the range is 1–128 times.

- **Password Lockout Policy**

- **Password Lock:** Once activated, the number of user login failures will be limited.
- **Lockout Threshold:** This value needs to be set when password lockout is enabled. If the number of incorrect entries exceeds the set range, the account will be locked and cannot be logged in again until it is unlocked. The range is 1 to 999 attempts.
- **Password Attempt Time Frame:** This value needs to be set when password lock is enabled. Within the set time frame, if the number of incorrect entries exceeds the password lock threshold, the user will be locked. The range is 1 to 99999 hours.
- **Auto-unlock time:** This value needs to be set when password lock is enabled. It represents the duration for which the lock will be maintained before automatic unlocking. The range is between 1 and 999999 minutes.

- **Captcha**

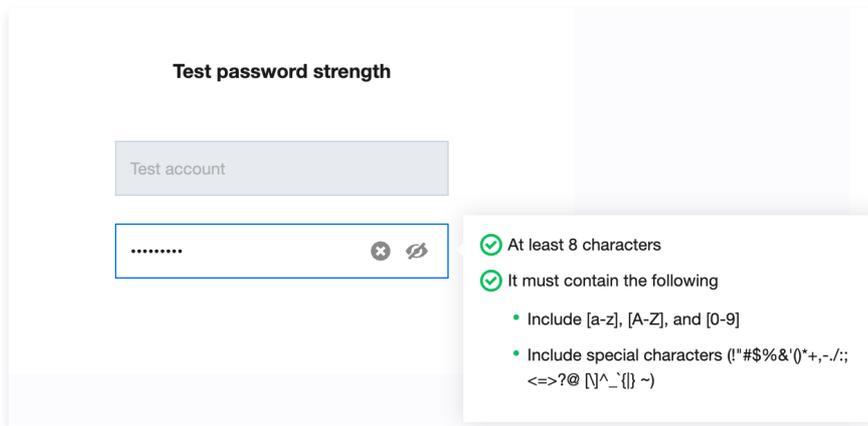
- **Verification Code:** Once enabled, if a user fails to log in for the specified consecutive number of times, verification code-based verification will be automatically activated.
- **Incorrect Password Count:** This value needs to be set when the verification code is enabled. If the number of incorrect entries exceeds the set range, verification code-based login verification will be initiated. The range is between 1 and 999 attempts.

**Note**

If password locking is enabled simultaneously, it is recommended to set a value here that is less than the lockout threshold, otherwise the user may be locked out before the verification code appears.

- **Test Password Strength**

After configuring the password policy, you can enter a test password to verify if it meets the password policy requirements.



**Test password strength**

Test account

.....

- ✓ At least 8 characters
- ✓ It must contain the following
  - Include [a-z], [A-Z], and [0-9]
  - Include special characters (!"#\$%&'()\*+,-./:;<=>?@[^\_`{|}~)

# SMS OTP

Last updated: 2023-09-04 10:34:17

## Scenario

The Account Risk Control Platform supports the use of SMS OTP as an authentication source, which verifies user identities through a combination of phone numbers and one-time verification codes.

## Instructions

1. Log in to the [Account Risk Control Platform console](#), and select **Authentication Management > General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, click **Create Authentication Source** to navigate to the Create Authentication Source page.
3. On the Create Authentication Source page, select **SMS OTP Authentication** and click **Next**.
4. On the Create Authentication Source page, set the authentication source icon, name, attributes, and description, then click **Next**.

### Note

- Authentication Source Icon: Displayed in the list and portal, users can click **Re-upload** to replace the default icon.
- Authentication Source Name: User Identity Authentication Source.
- Authentication Source Attribute: The SMS OTP authentication source defaults to using the user's mobile number attribute, which cannot be modified.
- Authentication Source Description: A brief overview of the authentication source.

1 Select an authentication method > 2 Configure authentication source > 3 Configure policy

Authentication source icon • auth\_message.svg

Select an image  
Delete

Upload a PNG or JPG file within 1 MB.

Authentication source name • SMS OTP

Authentication source attribute • Phone number

Authentication source description • Enter the description (up to 128 characters)

Back Next Cancel

5. On the Create Authentication Source page, configure the relevant parameters and click **OK** to create the authentication source.

### Note

- SMS Verification Code Length: This is a user-configured setting that determines the length of the verification code generated when a message is sent to the user, ranging from 1 to 6 digits.
- SMS Verification Code Validity: Users can configure the validity period of this verification code, ranging from 1 to 300 seconds.

- ✓ Select an authentication method
- >
- ✓ Configure authentication source
- >
- 3 Configure policy

**i** You can specify the length and validity of the SMS verification code. The default length is 6 digits and the validity is 60 seconds.

**Configure SMS policy**

Length of verification code \*  bit

Validity period of SMS verification code \*  seconds

[Back](#) [Cancel](#) [OK](#)

# Email OTP

Last updated: 2023-09-04 11:35:15

## Scenario

The Account Risk Control Platform supports the use of Email OTP as an authentication source, which verifies user identities through their email addresses and one-time verification codes.

## Instructions

1. Log in to the [Account Risk Control Platform console](#), select **Authentication Management > General Authentication Source** from the left navigation bar to access the General Authentication Source page.
2. On the General Authentication Source page, click **Create Authentication Source** to navigate to the Create Authentication Source page.
3. On the Create Authentication Source page, select **Email OTP Authentication** and click **Next**.
4. On the Create Authentication Source page, set the authentication source icon, name, attributes, and description, then click **Next**.

### Note

- Authentication Source Icon: Displayed in the list and portal, users can click **Re-upload** to replace the default icon.
- Authentication Source Name: User Identity Authentication Source.
- Authentication Source Attribute: The Email OTP Authentication Source defaults to using the email address attribute, which cannot be altered.
- Authentication Source Description: A brief overview of the authentication source.

Progress: 1. Select an authentication method (checked) > 2. Configure authentication source (active) > 3. Configure policy

Authentication source icon:  auth\_email.svg  
Buttons: Select an image, Delete  
Note: Upload a PNG or JPG file within 1 MB.

Authentication source name:

Authentication source attribute:

Authentication source description:

Buttons: Back, Next, Cancel

5. On the Create Authentication Source page, configure the relevant parameters and click **OK** to create the authentication source.

### Note

- Email Verification Code Length: The user-configured length of the verification code generated when sending emails to users, ranging from 1 to 128 characters.
- Email Verification Code Validity: Users can configure the validity period of this verification code, ranging from 1 to 300 seconds.

✓ Select an authentication method > ✓ Configure authentication source > 3 Configure policy

**i** You can specify the length of the email OTP and the validity. The default verification code length is 6 digits, and the validity period is 60 seconds.

**Configure email OTP policy**

Email verification code length \*  bit

Email verification code validity \*  seconds

[Back](#) [Cancel](#) [OK](#)

# Editing an authentication source

## Account and Password Authentication

Last updated: 2023-09-04 11:37:33

### Preparations

The enabled authentication source cannot be edited. It must be disabled before any modifications can be made.

### Instructions

1. Log in to the [Account Risk Control Platform console](#), and select **Authentication Management > General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, select the desired authentication source and click **Edit** to access the editing page.

| Authentication source name/ID   | Description | On/Off                   | Operation                                   |
|---|-------------|--------------------------|---|
|  Email OTP<br>.....                        | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |
|  SMS OTP<br>.....                          | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |
|  Username-password authentication<br>..... | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |

Total items: 3

10 / page

3. On the Basic Information page, modify the basic information as needed and click **Confirm** to update the basic information.

#### ← Edit Username-password authentication

**Basic information**    Configure policy

Authentication source icon \*    auth\_accountpasswo...

  
[Select an image](#)  
[Delete](#)

Upload a PNG or JPG file within 1 MB.

Authentication source name \*    Username-password authentication

Authentication source attribute \*    Username

Authentication source description    Enter the description (up to 128 characters)

4. Click on **Password Policy** to switch to the page for editing the password policy of account password authentication.
5. On the Password Policy page, modify the authentication source policy and click **OK** to change the authentication source password policy.

#### Note

For parameters related to the authentication source password policy, please refer to [Configuration Policy Parameter Description](#).

# SMS OTP

Last updated: 2023-09-04 10:34:52

## Preparations

The enabled authentication source cannot be edited. It must be disabled before any modifications can be made.

## Instructions

1. Log in to the [Account Risk Control Platform console](#), and select **Authentication Management > General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, select SMS OTP Authentication and click **Edit** to access the Basic Information page for SMS OTP Authentication.

| Authentication source name/ID   | Description | On/Off                   | Operation                                   |
|---|-------------|--------------------------|---|
|  Email OTP<br>.....                        | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |
|  SMS OTP<br>.....                          | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |
|  Username-password authentication<br>..... | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |

3. On the Basic Information page, modify the basic information as needed and click **Confirm** to update the basic information.

← **Edit SMS OTP**

**Basic information**    Configure policy

---

Authentication source icon \*    auth\_message.svg

  
[Delete](#)

Upload a PNG or JPG file within 1 MB.

Authentication source name \*    SMS OTP

Authentication source attribute \*    Phone number 

Authentication source description    Enter the description (up to 128 characters)

4. Click on **SMS Policy** to switch to the SMS Policy page for editing SMS OTP Authentication.
5. On the SMS Policy page, modify the authentication source policy and click **OK** to update the SMS policy for the authentication source.

### Note

- **SMS Verification Code Length:** This is a user-configured setting that determines the length of the verification code generated when a message is sent to the user, ranging from 1 to 6 digits.
- **SMS Verification Code Validity:** Users can configure the validity period of this verification code, ranging from 1 to 300 seconds.

 You can specify the length and validity of the SMS verification code. The default length is 6 digits and the validity is 60 seconds.

**Configure SMS policy**

Length of verification code \*    bit

Validity period of SMS verification code \*    seconds

# Email OTP

Last updated: 2023-09-04 11:42:26

## Preparations

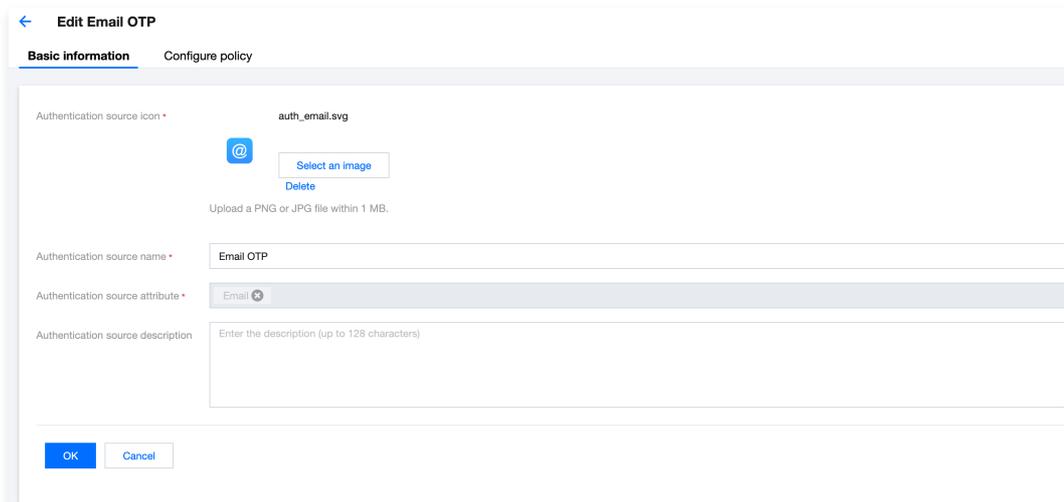
The enabled authentication source cannot be edited. It must be disabled before any modifications can be made.

## Instructions

1. Log in to the [Account Risk Control Platform console](#), and select **Authentication Management > General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, select Email OTP Authentication and click **Edit** to access the basic information editing page for Email OTP Authentication.

| Authentication source name/ID   | Description | On/Off                   | Operation                                   |
|---|-------------|--------------------------|---|
|  Email OTP<br>.....                        | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |
|  SMS OTP<br>.....                          | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |
|  Username-password authentication<br>..... | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |

3. On the Basic Information page, modify the basic information as needed and click **Confirm** to update the basic information.



4. Click on **Email Policy** to switch to the Email OTP Authentication policy editing page.
5. On the Email Policy page, modify the email verification code length and validity period, then click **OK** to update the authentication source email policy.

### Note

- **SMS Verification Code Length:** This is a user-configured setting that determines the length of the verification code generated when a message is sent to the user, ranging from 1 to 6 digits.
- **SMS Verification Code Validity:** Users can configure the validity period of this verification code, ranging from 1 to 300 seconds.

 You can specify the length of the email OTP and the validity. The default verification code length is 6 digits, and the validity period is 60 seconds.

**Configure email OTP policy**

Email verification code length    bit

Email verification code validity    seconds

OK

Cancel

# Testing an authentication source

Last updated: 2023-09-04 10:36:45

## Test SMS

1. Log in to the [Account Risk Control Platform console](#), and select **Authentication Management > General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, select SMS OTP Authentication, and click **Test SMS** to open the Test SMS pop-up window.

### Note

The Test SMS feature is only available when the SMS OTP Authentication source is enabled.

| Authentication source name/ID  | Description | On/Off                              | Operation                   |
|--|-------------|-------------------------------------|-----------------------------|
|  SMS OTP                          | -           | <input checked="" type="checkbox"/> | Edit Delete <b>Test SMS</b> |
|  Email OTP                        | -           | <input type="checkbox"/>            | Edit Delete                 |
|  Username-password authentication | -           | <input type="checkbox"/>            | Edit Delete                 |

3. In the Test SMS pop-up window, enter the mobile number and click **Send Test SMS**. A test SMS will be sent to the user based on the configuration of the SMS OTP Authentication source.

**Test SMS** ×

Mobile number \*

## Test email

1. Log in to the [Account Risk Control Platform console](#), and select **Authentication Management > General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, select Email OTP Authentication Source, and click **Test Email** to open the Test Email pop-up window.

### Note

The Test Email feature is only available when the Email OTP Authentication source is enabled.

| Authentication source name/ID  | Description | On/Off                              | Operation                     |
|--|-------------|-------------------------------------|-------------------------------|
|  Email OTP                        | -           | <input checked="" type="checkbox"/> | Edit Delete <b>Test email</b> |
|  SMS OTP                          | -           | <input checked="" type="checkbox"/> | Edit Delete Test SMS          |
|  Username-password authentication | -           | <input type="checkbox"/>            | Edit Delete                   |

3. In the Test Email pop-up window, enter the email address and click **Send Test Email**. A test email will be sent to the user based on the configuration of the Email OTP Authentication source.

# Disabling or deleting an authentication source

Last updated: 2023-09-04 10:36:50

## Scenario

This document outlines the process of disabling and deleting an authentication source in the Account Risk Control console.

### Note

- Upon disabling the authentication source, the application's ability to utilize this source will be affected. Please proceed with caution.
- Please be aware that all data will be irretrievable once the authentication source is deleted. Proceed with caution.

## Disabling Authentication Source

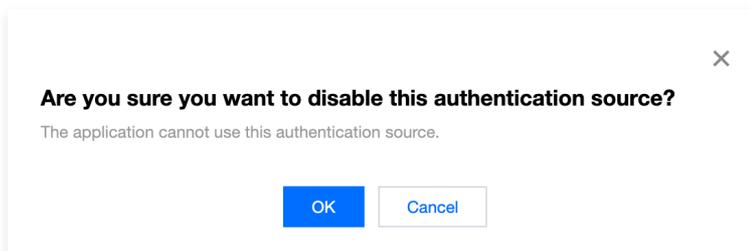
1. Log in to the [Account Risk Control Platform console](#), and select **Authentication Management > General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, select the required authentication source and click  to trigger the "Confirm Closure" pop-up window.

| Authentication source name/ID   | Description | On/Off  | Operation              |
|---|-------------|---|------------------------|
|  Email OTP<br>.....                          | -           |    | Edit Delete Test email |
|  SMS OTP<br>.....                            | -           |    | Edit Delete Test SMS   |
|  Username-password authentication<br>..... | -           |  | Edit Delete            |

3. In the "Confirm Closure" pop-up window, click **Confirm** to disable the authentication source.

### Note

- If the authentication source is set as the preferred source in the application's login process, a prompt will appear indicating that it cannot be disabled. If you wish to proceed with disabling, you may do so after unbinding the process in the application flow, and then proceed to disable the authentication source.
- If the authentication source is set as an associated source in the application's login process, a prompt will appear after disabling the source, indicating that the application's use of the authentication source will be affected.



## Deleting Authentication Source

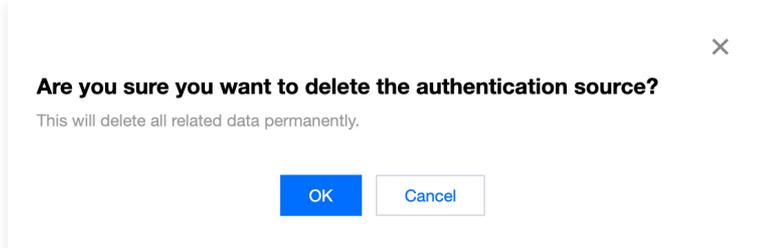
1. Log in to the [Account Risk Control Platform console](#), and select **Authentication Management > General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, select the desired authentication source, click Delete, and a "Confirm Deletion" pop-up window will appear.

### Note

If the authentication source is set as the preferred source in the application's login process, a prompt will appear indicating that it cannot be disabled. If you wish to proceed with disabling, you may do so after unbinding the process in the application flow, and then proceed to disable the authentication source.

| Authentication source name/ID   | Description | On/Off                              | Operation              |
|---|-------------|-------------------------------------|------------------------|
|  Email OTP<br>.....                        | -           | <input checked="" type="checkbox"/> | Edit Delete Test email |
|  SMS OTP<br>.....                          | -           | <input checked="" type="checkbox"/> | Edit Delete Test SMS   |
|  Username-password authentication<br>..... | -           | <input type="checkbox"/>            | Edit <b>Delete</b>     |

3. In the "Confirm Deletion" pop-up window, click confirm to delete the authentication source.



# SNS authentication source

## Creating an authentication source

### PC WeChat Login

Last updated: 2023-09-04 10:36:57

#### Scenario

Supports users to swiftly log in to the application using their WeChat identity via QR code scanning.

#### Instructions

1. Log in to the [Account Risk Control Console](#), and select **Authentication Management > Social Authentication Source** from the left navigation bar.
2. On the Social Authentication Source page, click **Create Authentication Source** to navigate to the Create Authentication Source page.
3. On the Create Authentication Source page, select PC WeChat Login, and click **Next**.
4. On the Create Authentication Source page, after setting the relevant parameters, click **OK** to create the authentication source.

Progress: 1. Select an authentication source type (Completed) > 2. Configure authentication source (Current) > 3. Complete

Authentication source icon: Select an image Delete

Upload a PNG or JPG file within 1 MB.

Authentication source name: WeChat for PC

Authentication source description: Enter the description (up to 128 characters)

AppID: Enter the AppID  
Go to WeChat Open Platform and choose "Webpage Applications". Click your application to get the AppID.

AppSecret: Enter the AppSecret  
Go to WeChat Open Platform and choose "Webpage Applications". Click your application to get the AppSecret.

Attribute mapping:

| Authentication source attribute | CIAM attribute |
|---------------------------------|----------------|
| openid                          | wechatOpenId   |
| unionid                         | wechatUnionId  |

⊕ Add

Buttons: Back, OK, Cancel

#### Parameters:

- Authentication Source Icon: Displayed in the list and portal, users can click **Re-upload** to replace the default icon.
- Authentication Source Name: A user identifier for the authentication source, which is a required field.
- Authentication Source Description: A brief description of the authentication source, not mandatory.
- AppID: Visit the [WeChat Open Platform](#) web application page and click **View** to obtain the AppID.
- AppSecret: Visit the Web Application page of the [WeChat Open Platform](#), click **View** to obtain the AppSecret.
- Attribute Mapping: This is used to map the attributes returned during the WeChat authentication process to the attributes defined by the platform. By default, it includes two uneditable attribute mappings: openid and unionid. Click **Add** to establish a new mapping relationship. The source attribute name is the WeChat attribute, and the platform attribute is the attribute defined in the custom attributes.

# WeChat webpage login

Last updated: 2023-09-04 10:37:04

## Scenario

Enables users to swiftly log into the application by confirming WeChat authorization within a WeChat webpage.

## Instructions

1. Log in to the [Account Risk Control Console](#), and select **Authentication Management > Social Authentication Source** from the left navigation bar.
2. On the Social Authentication Source page, click **Create Authentication Source** to navigate to the Create Authentication Source page.
3. On the Create Authentication Source page, select **WeChat Web Login** and click **Next**.
4. On the Create Authentication Source page, after setting the relevant parameters, click **OK** to create the authentication source.

Progress: 1. Select an authentication source type (Completed) > 2. Configure authentication source (Current) > 3. Complete

Authentication source icon:  auth\_wxaccount.svg  
Buttons: Select an image, Delete  
Upload a PNG or JPG file within 1 MB.

Authentication source name: WeChat webpage login

Authentication source description: Enter the description (up to 128 characters)

AppID: Enter the AppID  
Go to WeChat Official Account Platform and choose "Settings and Development" -> "Basic Configuration". Click your application to get the AppID.

AppSecret: Enter the AppSecret  
Go to WeChat Official Account Platform and choose "Settings and Development" -> "Basic Configuration". Click your application to get the AppSecret.

Scope:  snsapi\_userinfo  snsapi\_base

Business domain name verification file: Select a file  
The file cannot exceed 1M. To download the verification file, please go to the WeChat Official Accounts Platform, and select "Settings and Development" -> "Account Info" -> "Function setting" -> "Webpage authorization domain name".

Name of the business domain name verification file: [Empty field]

Business domain name verification file content: [Empty field]

Attribute mapping:

| Authentication source attribute | CIAM attribute |
|---------------------------------|----------------|
| openid                          | wechatOpenId   |
| unionid                         | wechatUnionid  |

Buttons: Back, OK, Cancel

### Parameters:

- Authentication Source Icon: Displayed in the list and portal, users can click **Re-upload** to replace the default icon.
- Authentication Source Name: A user identifier for the authentication source, which is a required field.
- Authentication Source Description: A brief description of the authentication source, not mandatory.
- AppID: On the [WeChat Open Platform](#) webpage application page, click **View** to obtain the AppID.
- AppSecret: On the [WeChat Open Platform](#) webpage application page, click **View** to obtain the AppSecret.
- Scope: You can choose to initiate webpage authorization with either `snsapi_userinfo` or `snsapi_base` as the scope.
  - `snsapi_userinfo`: Used to obtain the openid of the user entering the page, silently authorizes and automatically redirects to the callback page.
  - `snsapi_base`: Utilized to retrieve basic user information. This authorization requires manual user consent, and upon approval, the user's basic information is obtained.

- Business Domain Verification File: When modifying the web authorization domain on the WeChat Public Platform, for security purposes, a file from the developer's web server is required. The file can be obtained from [WeChat Public Platform](#) > **Settings and Development** > **WeChat Official Account Settings** > **Functional Settings** > **Web Authorization Domain**. Click **Settings** to download the file in the pop-up box.



- Business Domain Verification File Name: The file name is automatically filled in after the file is uploaded.
- Business Domain Verification File Content: The file content is automatically filled in after the file is uploaded.
- Attribute Mapping: This is used to map the attributes returned during the WeChat authentication process to the attributes defined by the platform. By default, it includes two uneditable attribute mappings: openid and unionid. Click **Add** to establish a new mapping relationship. The source attribute name is the WeChat attribute, and the platform attribute is the attribute defined in the custom attributes.

# WeChat Mini Program login

Last updated: 2023-09-04 10:37:10

## Scenario

Enables users to swiftly log into the application within the Mini Program by confirming authorization via WeChat, utilizing their WeChat identity.

## Instructions

1. Log in to the [Account Risk Control Console](#), and select **Authentication Management > Social Authentication Source** from the left navigation bar.
2. On the Social Authentication Source page, click **Create Authentication Source** to navigate to the Create Authentication Source page.
3. On the Create Authentication Source page, select **WeChat Mini Program Login** and click **Next**.
4. On the Create Authentication Source page, after setting the relevant parameters, click **OK** to create the authentication source.

The screenshot shows the 'Configure authentication source' step of the 'Create Authentication Source' process. The progress bar at the top indicates the current step is '2. Configure authentication source'. The form contains the following fields and options:

- Authentication source icon:** A circular icon with a document symbol, labeled 'auth\_wxapplet.svg'. Below it are 'Select an image' and 'Delete' buttons.
- Authentication source name:** A text input field containing 'WeChat Mini Program login'.
- Authentication source description:** A text input field with a placeholder 'Enter the description (up to 128 characters)'.
- AppID:** A text input field with a placeholder 'Enter the AppID'. Below it is a note: 'To check the WeChat Mini Program ID, please go to WeChat Mini Program -> Development Management -> Development Settings.'
- AppSecret:** A text input field with a placeholder 'Enter the AppSecret'. Below it is a note: 'To check the WeChat Mini Program secret, please go to WeChat Mini Program -> Development Management -> Development Settings.'
- Business domain name verification file:** A file upload area with a 'Select a file' button. Below it is a note: 'Please upload a TXT file within 1 MB.'
- Name of the business domain name verification file:** A text input field with a note: 'If you need to call the login page managed by CIAM by using webview, you need to upload the checksum file provided by the Mini Program.'
- Business domain name verification file content:** A text input field with a note: 'If you need to call the login page managed by CIAM by using webview, you need to upload the checksum file provided by the Mini Program.'
- Attribute mapping:** A table with two columns: 'Authentication source attribute' and 'CIAM attribute'.

| Authentication source attribute | CIAM attribute |
|---------------------------------|----------------|
| openid                          | wechatOpenid   |
| unionid                         | wechatUnionid  |

At the bottom left, there are 'Back', 'OK', and 'Cancel' buttons. An 'Add' button is also visible below the attribute mapping table.

## Parameters:

- **Authentication Source Icon:** Displayed in the list and portal, users can click **Re-upload** to replace the default icon.
- **Authentication Source Name:** A user identifier for the authentication source, which is a required field.
- **Authentication Source Description:** A brief description of the authentication source, not mandatory.
- **AppID:** Go to [WeChat Mini Program Platform](#) > **Development Management** > **Development Settings**, click **View** to see the Mini Program ID.
- **AppSecret:** Go to [WeChat Mini Program Platform](#) > **Development Management** > **Development Settings**, click **View** to see the Mini Program key.
- **Business Domain Verification File:** When modifying the web authorization domain on the WeChat Public Platform, for security purposes, a file from the developer's web server is required. The file can be obtained from [WeChat Mini Program Platform](#) > **Development** > **Development Management** > **Development Settings** > **Business Domain**. Click **Settings** to download the file in the pop-up box.
- **Business Domain Verification File Name:** The file name is automatically filled in after the file is uploaded.
- **Business Domain Verification File Content:** The file content is automatically filled in after the file is uploaded.

- **Attribute Mapping:** This is used to map the attributes returned during the WeChat authentication process to the attributes defined by the platform. By default, it includes two uneditable attribute mappings: openid and unionid. Click **Add** to establish a new mapping relationship. The source attribute name is the WeChat attribute, and the platform attribute is the attribute defined in the custom attributes.

## QQ login

Last updated: 2023-09-04 10:37:16

## Scenario

Allows the end user to swiftly log in to the application using QQ authentication.

### Create authentication source

1. Log in to the [Account Risk Control Console](#), and select **Authentication Management** > **Social Authentication Source** from the left navigation bar.
2. On the Social Authentication Source page, click **Create Authentication Source** to navigate to the Create Authentication Source page.
3. On the Create Authentication Source page, select **QQ Login** and click **Next**.
4. On the Create Authentication Source page, configure the relevant parameters and click **OK** to create the authentication source.

The screenshot shows the 'Configure authentication source' step of a three-step process. The page is titled 'auth\_qq.png' and features a penguin icon. Below the icon is a 'Select an image' button and a 'Delete' button. A note indicates that users should upload a PNG or JPG file within 1 MB. The form includes several input fields: 'Authentication source name' (pre-filled with 'Log in via QQ'), 'Authentication source description' (with a placeholder 'Enter the description (up to 128 characters)'), 'AppID' (with a placeholder 'Enter the AppID' and a note to go to QQ Open Platform), and 'App Key' (with a placeholder 'Enter the APP Key' and a note to go to QQ Open Platform). An 'Attribute mapping' section contains two columns: 'Authentication source attribute' and 'CIAM attribute'. The first row maps 'openid' to 'qqOpenId', and the second row maps 'unionid' to 'qqUnionId'. An 'Add' button is located below the mapping table. At the bottom of the form are 'Back', 'OK', and 'Cancel' buttons.

#### Parameter description:

- **Authentication Source Icon:** Displayed in the list and portal, users can click **Re-upload** to replace the default icon.
- **Authentication Source Name:** A user identifier for the authentication source, which is a required field.
- **Authentication Source Description:** A brief description of the authentication source, not mandatory.
- **APP ID:** Visit [QQ Open Platform](#) > **Application Management** > **Create Application** to obtain the APP ID (also known as clientID).
- **APP Key:** Visit [QQ Open Platform](#) > **Application Management** > **Create Application** to obtain the APP Key (also known as client secret).
- **Attribute Mapping:** This is used to map the attributes returned during the QQ authentication process to the attributes defined by the platform. By default, it includes two uneditable attribute mappings: openid and unionid. Click **Add** to establish a new mapping relationship. The authentication source attribute name is the QQ authentication source attribute, and the platform attribute is the attribute defined in attribute customization.

### Creating an application

For detailed instructions on creating an application on the [QQ Open Platform](#), please refer to the [Create Application Documentation](#). If you are using a domain provided by CIAM, please fill in the information as per the following requirements:

| Parameter name           | Enter Details   |
|--------------------------|---|
| Website Domain           | https://{domain prefix}.prod.tencentciam.com  |
| Website Callback Address | https://{domain prefix}.prod.tencentciam.com/login/oauth2/code/{authentication source id} |
| Provider                 | Shenzhen Tencent Computer Systems Co., Ltd.   |
| ICP Filing Number        | YueB2-20090059  |

**Note**

Where {} is a placeholder that needs to be replaced with the actual content.

# Alipay Login

Last updated: 2023-09-04 10:37:27

## Scenario

Allows the end user to swiftly log in to the application using Alipay authentication.

## Instructions

1. Log in to the [Account Risk Control Console](#), and select **Authentication Management > Social Authentication Source** from the left navigation bar.
2. On the Social Authentication Source page, click **Create Authentication Source** to navigate to the Create Authentication Source page.
3. On the Create Authentication Source page, select Alipay Login and click **Next**.
4. On the Create Authentication Source page, after setting the relevant parameters, click **OK** to create the authentication source.

The screenshot shows the 'Configure authentication source' page for Alipay Login. The page is divided into three steps: 'Select an authentication source type' (completed), 'Configure authentication source' (current), and 'Complete'. The form includes the following fields and options:

- Authentication source icon:** A default Alipay icon is shown. There are 'Select an image' and 'Delete' buttons. Below the icon, it says 'Upload a PNG or JPG file within 1 MB.'
- Authentication source name:** A text input field containing 'Alipay'.
- Authentication source description:** A text area for entering a description (up to 128 characters).
- AppID:** A text input field for entering the AppID. A note below says: 'To get the AppID, please go to the Alipay Open Platform console and create the application first.'
- Attribute mapping:** A table with two columns: 'Authentication source attribute' and 'CIAM attribute'. A row shows 'user\_id' mapped to 'alipayUserId'. There is an 'Add' button below the table.
- Alipay public key:** A text area for entering the application public key provided by Alipay. A note below says: 'To check the API encryption method, please go to the Alipay Open Platform console and select "Application Information -> Opening settings".'
- Application private key:** A text area for entering the application private key provided by Alipay. A note below says: 'It's added to the code for the signature. The developer can generate it by using the Alipay key generator and keep it on their own.'
- Signature algorithm:** A dropdown menu set to 'RSA2'. A note below says: 'The algorithm used by the merchant to generate the signature'.

At the bottom of the form, there are three buttons: 'Back', 'OK', and 'Cancel'.

### Parameters:

- **Authentication Source Icon:** Displayed in the list and portal, users can click **Re-upload** to replace the default icon.
- **Authentication Source Name:** A user identifier for the authentication source, which is a required field.
- **Authentication Source Description:** A brief description of the authentication source, not mandatory.
- **AppID:** Visit [Alipay Open Platform](#) > **Console** > **Create Application**. After creating the application, you can obtain the AppID.
- **Attribute Mapping:** This is used to map the attributes returned during the Alipay authentication process to the attributes defined by the platform. The Alipay authentication source includes a default user\_id attribute mapping. Click **Add** to establish a new mapping relationship. The authentication source attribute name is the Alipay attribute, and the platform attribute is the attribute defined in the custom attributes.
- **Alipay Public Key:** Visit [Alipay Open Platform](#) > **Console** > **Application Information** > **Open Settings** to view the interface encryption method and obtain the key.
- **Application Private Key:** Retained by the developer and required to be entered into the code for signing purposes. The developer can generate this using the Alipay Key Generation Tool.
- **Signature Algorithm:** The type of algorithm used by the merchant to generate the signature string, default is RSA2.

# Editing an authentication source

Last updated: 2023-09-04 10:38:48

## Preparations

The enabled authentication source cannot be edited. It must be disabled before any modifications can be made.

## Instructions

1. Log in to the [Account Risk Control Console](#), and select **Authentication Management > Social Authentication Source** from the left navigation bar.
2. On the Social Authentication Source page, select the desired authentication source and click **Edit** to navigate to the editing page.

| Authentication source name/ID   | Description | On/Off                   | Operation                                   |
|---|-------------|--------------------------|---|
|  Alipay                    | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |
|  Log in via QQ             | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |
|  WeChat Mini Program login | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |
|  WeChat for PC             | -           | <input type="checkbox"/> | <a href="#">Edit</a> <a href="#">Delete</a> |

3. On the editing page, you can modify parameters such as the authentication source icon, authentication source name, and authentication source description. Click **Confirm** to save the changes.

### Note

This document uses the editing of PC WeChat login as an example.

#### Edit WeChat for PC

Authentication source icon \* auth\_weixin.svg



Upload a PNG or JPG file within 1 MB.

Authentication source name \*

Authentication source description

AppID \*   
Go to WeChat Open Platform and choose "Webpage Applications". Click your application to get the AppID.

AppSecret \*   
Go to WeChat Open Platform and choose "Webpage Applications". Click your application to get the AppSecret.

Attribute mapping ⓘ \*

| Authentication source attribute      | CIAM attribute                             |
|--------------------------------------|--|
| <input type="text" value="openid"/>  | <input type="text" value="wechatOpenId"/>  |
| <input type="text" value="unionid"/> | <input type="text" value="wechatUnionId"/> |

# Disabling or deleting an authentication source

Last updated: 2023-09-04 10:38:56

## Scenario

This document outlines the process of disabling and deleting an authentication source in the Account Risk Control console.

### Note

- Upon disabling the authentication source, the application's ability to utilize this source will be affected. Please proceed with caution.
- Please be aware that all data will be irretrievable once the authentication source is deleted. Proceed with caution.

## Disabling Authentication Source

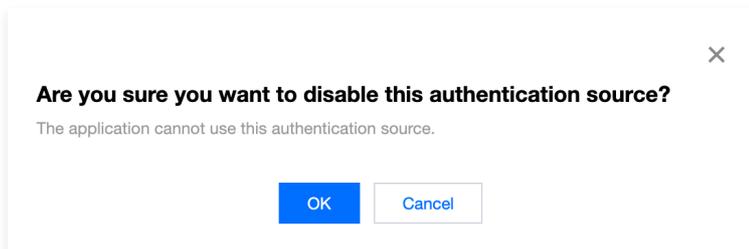
1. Log in to the [Account Risk Control Console](#), and select **Authentication Management** > **Social Authentication Source** from the left navigation bar.
2. On the Social Authentication Source page, select the desired authentication source and click  to trigger the "Confirm Closure" pop-up window.

| Authentication source name/ID   | Description | On/Off  | Operation   |
|---|-------------|---|-------------|
|  Alipay                      | -           |    | Edit Delete |
|  Log in via QQ               | -           |    | Edit Delete |
|  WeChat Mini Program login | -           |  | Edit Delete |
|  WeChat for PC             | -           |  | Edit Delete |

3. In the "Confirm Closure" pop-up window, click **Confirm** to disable the authentication source.

### Note

- If the authentication source is set as the preferred source in the application's login process, a prompt will appear indicating that it cannot be disabled. If you wish to proceed with disabling, you may do so after unbinding the process in the application flow, and then proceed to disable the authentication source.
- If the authentication source is set as an associated source in the application's login process, a prompt will appear after disabling the source, indicating that the application's use of the authentication source will be affected.



## Deleting Authentication Source

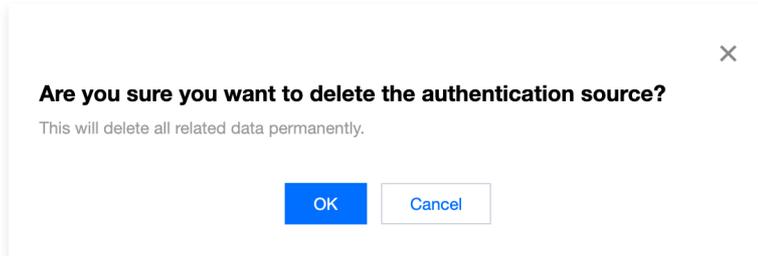
1. On the [Social Authentication Source](#) page, select the desired authentication source and click **Delete**. A confirmation pop-up window will appear.

### Note

When the authentication source is set as an associated source in the application's login process, deleting it will affect the application's use of the authentication source. Please ensure accuracy before proceeding with the deletion.

| Authentication source name/ID   | Description | On/Off                              | Operation          |
|---|-------------|-------------------------------------|--------------------|
|  Alipay                    | -           | <input checked="" type="checkbox"/> | Edit Delete        |
|  Log in via QQ             | -           | <input type="checkbox"/>            | Edit <b>Delete</b> |
|  WeChat Mini Program login | -           | <input type="checkbox"/>            | Edit Delete        |
|  WeChat for PC             | -           | <input type="checkbox"/>            | Edit Delete        |

2. In the "Confirm Deletion" pop-up window, click **Confirm** to delete the authentication source.



# Audit Management

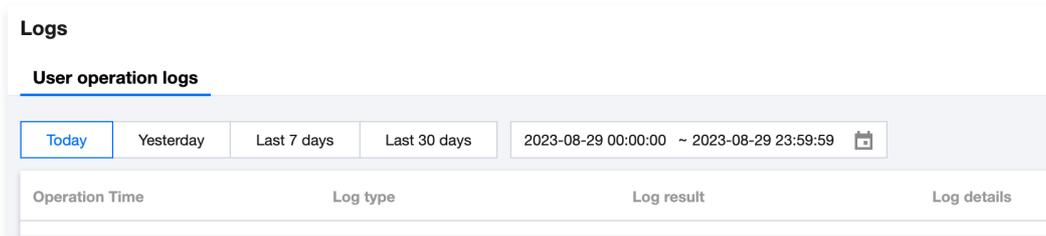
Last updated: 2023-09-04 10:39:06

## Scenario

Audit logs meticulously record the key operations performed by users on the platform. Administrators can review any record at any time, replay a specific operation, and tally high-risk behaviors. This document will guide you on how to view user operation logs in the Account Risk Control Platform console.

## Instructions

1. Log in to the [Account Risk Control Platform console](#), and select **Audit Management > User Operation Logs** from the left sidebar.
2. On the User Operation Logs page, you can view the logs by adjusting the time frame or using the search box.
  - Click to switch "Time", and select a date (today, yesterday, last 7 days, last 30 days) to view the logs.



- Enter the log type, log result, authentication source, and application in the search box, then click to find the logs.

| Operation Time      | Log type | Log result | Log details      | Authentication source            | Apply         | IP address |
|---------------------|----------|------------|------------------|----------------------------------|---------------|------------|
| 2023-08-29 19:03:25 | 登出       | 成功         | 登出成功。用户ID: ..... | -                                | First Web App | .....      |
| 2023-08-29 19:03:00 | 登录       | 成功         | 登录成功。用户ID: ..... | Username-password authentication | First Web App | .....      |

# Custom Settings

## Template Configuration

### SMS templates

Last updated: 2023-09-04 10:39:20

#### Scenario

By default, the Account Risk Control Platform provides each tenant with 50 free SMS messages. Once this quota is exceeded, the platform will suspend SMS delivery for the tenant, affecting console test messages, portal SMS OTP authentication, and MFA two-factor authentication. To ensure the normal operation of the business, administrators need to configure SMS templates to provide messaging services for platform operations.

#### Setting up SMS Templates

1. Log in to the [Account Risk Control Platform Console](#), and in the left navigation bar, click on **Personalized Settings > Template Settings > SMS Templates**.
2. On the SMS Templates page, if the current tenant has not configured an SMS template, the system will display the following blank template information by default, and the immediate SMS service testing function will be unavailable.

**SMS service configuration** [SMS service configuration guide](#)

SMS Service: Tencent Cloud SMS Service

SDK AppID

Secret ID

SecretKey

**Verification code SMS**

Registration verification  
Sample: Tencent Security: Your verification code is {1}. This code expires in {2} seconds. Be sure to keep it secret. Please ignore this message if you haven't requested any codes.

Login  
Example: [Tencent Security] Your SMS login verification code: {1}, valid for {2} seconds, please do not disclose it. If it is not done by me, please ignore

Two-step authentication  
Sample: Tencent Security: Your verification code is {1}. This code expires in {2} seconds. Be sure to keep it secret. Please ignore this message if you haven't requested any codes.

Modifying mobile number  
Example: [Tencent Security] Your modified mobile phone number verification code: {1}, valid for {2} seconds, please do not disclose. If it is not done by me, please ignore.

Retrieve password SMS verification code  
Example: [Tencent Security] Your SMS verification code for password recovery: {1}, valid for {2} seconds, please do not disclose it. If it is not done by me, please ignore

**SMS service test**

[Test now](#)

3. On the SMS Templates page, click **Edit** in the top-right corner of the interface.
4. On the editing page, set the relevant parameters for the SMS service configuration and SMS template configuration respectively, then click **OK**.

**SMS service configuration** [SMS service configuration guide](#)

- SMS Service:
- SDK AppID:
- Secret ID:
- SecretKey:

**Verification code SMS**

- Registration verification:    
Sample: Tencent Security: Your verification code is {1}. This code expires in {2} seconds. Be sure to keep it secret. Please ignore this message if you haven't requested any codes.
- Login:    
Example: [Tencent Security] Your SMS login verification code: {1}, valid for {2} seconds, please do not disclose it. If it is not done by me, please ignore
- Two-step authentication:    
Sample: Tencent Security: Your verification code is {1}. This code expires in {2} seconds. Be sure to keep it secret. Please ignore this message if you haven't requested any codes.
- Modifying mobile number:    
Example: [Tencent Security] Your modified mobile phone number verification code: {1}, valid for {2} seconds, please do not disclose. If it is not done by me, please ignore.
- Retrieve password SMS verification code:    
Example: [Tencent Security] Your SMS verification code for password recovery: {1}, valid for {2} seconds, please do not disclose it. If it is not done by me, please ignore

**SMS service test**

**Note:**

Different SMS services require different configuration parameters. Currently, the platform only supports **Tencent Cloud SMS Service**, but will gradually support the configuration of other SMS services. The following are the relevant parameters needed to configure Tencent Cloud SMS Service.

## SMS service configuration

### Obtaining the SDK AppID

- Log in to the [Tencent Cloud SMS Console](#), and in the left navigation bar, select **Application Management > Application List**.
- On the Application List page, click **Create Application**, enter the application name and description, and click **Create** to complete the application creation process.

**创建应用** ✕

应用名称\*

应用简介

0 / 300

不超过300字

- On the application list page, select the desired application and click  to obtain the SDK AppID for that application.



### Obtaining the SecretId and SecretKey

1. Log in to the [Access Management Console](#), and in the left navigation bar, select **Users > User List**.
2. On the User List page, select the desired sub-account and click on the **Username** to enter the User Details page.

| 用户名称 | 用户类型 | 账号ID | 创建时间 | 关联信息 | 操作      |
|------|------|------|------|------|---------|
| 主账号  | 主账号  |      |      |      | 授权 更多操作 |
| 子用户  | 子用户  |      |      |      | 授权 更多操作 |

3. On the User Details page, click on **API Key**, select the required key, and click to obtain the SecretId for that sub-account. Click on **Show**, and after successful identity verification, you can obtain the SecretKey for that sub-account.



### SMS Template Configuration

Setting up an SMS template requires obtaining the SMS signature and SMS template ID needed for SMS login. The acquisition method is as follows:

**Verification code SMS**

- Registration verification
 

Sample: Tencent Security: Your verification code is {1}. This code expires in {2} seconds. Be sure to keep it secret. Please ignore this message if you haven't requested any codes.
- Login
 

Example: [Tencent Security] Your SMS login verification code: {1}, valid for {2} seconds, please do not disclose it. If it is not done by me, please ignore
- Two-step authentication
 

Sample: Tencent Security: Your verification code is {1}. This code expires in {2} seconds. Be sure to keep it secret. Please ignore this message if you haven't requested any codes.
- Modifying mobile number
 

Example: [Tencent Security] Your modified mobile phone number verification code: {1}, valid for {2} seconds, please do not disclose. If it is not done by me, please ignore.
- Retrieve password SMS verification code
 

Example: [Tencent Security] Your SMS verification code for password recovery: {1}, valid for {2} seconds, please do not disclose it. If it is not done by me, please ignore

### Retrieving SMS Signature

1. Log in to the [SMS Service Console](#), and in the left navigation bar, select **Domestic SMS > Signature Management**.
2. On the Signature Management page, click **Create Signature**, fill in the relevant parameters, and then click **Confirm**.

← **创建签名** 如果您希望与工程师即时沟通交流，欢迎通过腾讯云短信小助手联系我们，[点击进入对话](#)

\*您目前为个人认证用户，查看签名所需上传的证明材料：[自用](#)、[他用](#)\*

签名用途  自用 (签名为本账号实名认证的网站、APP、公众号、小程序等)  
 他用 (签名为非本账号实名认证的公司、网站、产品名等)

签名类型\*

签名内容\*   
长度为2~12字，由中英文、数字组成，内容不包含【】，范例：腾讯云。

申请说明   
0 / 300

请输入签名申请用途 (选填)

- 签名提交后，预计2小时完成审核。
- 审核工作时间:周一至周五 9:00-23:00 (法定节假日正常服务)。

3. After approval, you can view the SMS signature on the Signature Management page.

| ID | 内容 | 状态/原因 | 申请时间    | 操作 |
|----|----|-------|---------|----|
|    |    | 已通过   | 2020-1  | 删除 |
|    |    | 已通过   | 2020-05 | 删除 |

### Retrieving SMS Template ID

1. Log in to the [SMS Service Console](#), and in the left navigation bar, select **Domestic SMS** > **Body Template Management**.
2. On the Body Template Management page, click **Create Body Template**, fill in the relevant parameters, and click **OK** to confirm.

← **创建正文模板** 如果您希望与工程师即时沟通交流，欢迎通过腾讯云短信小助手联系我们，[点击进入对话](#)

模板名称\*

短信类型  普通短信  营销短信 [升级到企业认证后启用](#)

短信内容\*  支持自定义模板内容和使用标准模板，使用标准模板可提高审核效率和成功率。

模板示例：(1)为您的登录验证码，请于(2)分钟内填写。如非本人操作，请忽略本短信。（其中(数字)为可自定义的内容，须从1开始连续编号，如(1)、(2)等）

0 / 490

当前模板预计发送条数约为 0 条短信  
(实际发送时，签名和模板变量会影响计费条数，请特别关注)

申请说明

0 / 300

- 模板提交后，预计2小时完成审核。
- 审核工作时间:周一至周日 9:00-23:00 (法定节假日正常服务)。

3. Once approved, you can view the SMS template ID on the Body Template Management page.

| ID                   | 模板类型 | 模板名称                 | 内容                          | 状态/原因                                   | 申请时间                          | 操作  |
|----------------------|------|----------------------|-----------------------------|---|-------------------------------|---|
| <input type="text"/> | 普通短信 | <input type="text"/> | 验证码为：(1)，您正在登录，若非本人操作，请勿泄露。 | 已通过 <input checked="" type="checkbox"/> | 2020-05- <input type="text"/> | <a href="#">删除</a> <a href="#">复制到国际模板</a> <a href="#">群发</a> |
| <input type="text"/> | 普通短信 | <input type="text"/> | 验证码为：(1)，您正在登录，若非本人操作，请勿泄露。 | 已通过 <input checked="" type="checkbox"/> | 2020-05- <input type="text"/> | <a href="#">删除</a> <a href="#">复制到国际模板</a> <a href="#">群发</a> |
| <input type="text"/> | 普通短信 | <input type="text"/> | 您的验证码是(1)。                  | 未通过 <input type="checkbox"/>            | 2019-08- <input type="text"/> | <a href="#">查看失败原因并修改</a> <a href="#">删除</a>                  |

## Testing SMS Service

Users can test the validity and accuracy of the SMS service. The testing process is as follows.

1. On the SMS Template Configuration Edit page, click on **Test SMS Service Now** to open the test window.

**SMS service test**

2. In the SMS Service Test window, enter the mobile number and click **Send**. You can confirm whether the SMS service is configured correctly by checking if the entered mobile number receives the test SMS and SMS signature.

**SMS service test** ✕

• Mobile number +86 ▼ Enter the mobile number

• Test template  Registration verification  Login  Two-factor authentication  
 Modifying mobile number  Reset password

Send

3. After saving the SMS template configuration, you can verify the correctness of the configuration by clicking **Test SMS Service Now** on the SMS template view page.

The screenshot shows the 'Verification code SMS' configuration interface. A modal dialog titled 'SMS service test' is open, allowing the user to test the configuration. The dialog includes a mobile number dropdown menu currently set to '+86', an input field for the mobile number, and five radio button options for the test template: 'Registration verification' (selected), 'Login', 'Two-factor authentication', 'Modifying mobile number', and 'Reset password'. A blue 'Send' button is located at the bottom center of the dialog. In the background, the 'SMS service test' button on the main configuration page is highlighted with a red rectangular border.

# Email templates

Last updated: 2023-09-04 10:39:27

## Scenario

The Account Risk Control Platform by default provides each tenant with 50 complimentary emails. If this free quota is exceeded, the platform will temporarily suspend email sending for the tenant, affecting console test email OTP, portal email OTP authentication source login, and MFA two-factor authentication. To ensure the normal operation of the business, administrators need to configure email templates to guarantee the platform's regular email dispatch.

## Email Template Configuration

1. Log in to the [Account Risk Control Platform console](#), and in the left sidebar, click on **Personalized Settings > Template Settings > Email Template**.
2. On the Email Template page, if the current tenant has not configured an email template, the system will display the following blank template information by default. The 'Test Email Service' function is not available.

The screenshot displays the 'Email template' configuration page. At the top, there are tabs for 'SMS message template', 'Email template' (selected), 'Identity verification template', and 'Image CAPTCHA'. The main content is divided into two sections: 'Email service configuration' and 'Email header template configuration'. Under 'Email service configuration', there is a dropdown for 'Email service' set to 'Tencent Message Push', and input fields for 'Secret ID' and 'SecretKey'. Under 'Email header template configuration', there are several rows, each with a title, a text input field, and a reference template. The rows are: 'Registered Title', 'Login Title', 'Secondary Authentication Title', 'Update mailbox title', 'Retrieve password title', and 'Retrieve username title'. Each row includes a note about placeholder usage and a reference template example.

3. On the Email Template page, click **Edit** in the top-right corner of the interface.
4. On the editing page, set the relevant parameters for the email service configuration and email template configuration respectively, then click **OK**.

### Note

Different email services require different configuration parameters. Currently, the platform **only supports Tencent Email Push**, but will gradually support the configuration of other email services. The following are the relevant parameters needed to configure the Tencent Cloud Email Service.

## Email Service Configuration

Email template configuration supports different email gateways. By selecting a supported email service, the page will dynamically load the configuration information required for that email service.

## Obtaining the SecretId and SecretKey

1. Log in to the [Access Management Console](#), and in the left sidebar, click on **Users > User List**.
2. On the User List page, select the desired sub-account and click on the **Username** to enter the User Details page.

| 用户名称 | 用户类型 | 账号ID | 创建时间 | 关联信息 | 操作      |
|------|------|------|------|------|---------|
| 主账号  | 主账号  |      |      |      | 授权 更多操作 |
| 子用户  | 子用户  |      |      |      | 授权 更多操作 |

3. On the User Details page, click on **API Key**, select the required key, and click  to obtain the SecretId for that sub-account. Click on **Show**, and after successful identity verification, you can obtain the SecretKey for that sub-account.

| API 密钥   | 创建时间 | 最近访问时间     | 状态  | 操作 |
|--|------|------------|-----|----|
| SecretId: AI<br>SecretKey: *****<br><a href="#">显示</a> | 2    | 2021-06-15 | 已启用 | 禁用 |

## Obtain Sender Address

1. Log in to the [Email Push Console](#), and in the left sidebar, click on **Email Configuration > Sender Domain**.
2. On the Sender Domain page, click **Create Domain**, enter the domain name, which will be used to create the sender address, and click **Submit**. For detailed configuration, refer to [Sender Domain](#).

**新建发信域名** ✕

域名

不可使用企业邮箱域名, 以免产生SPF、MX记录的冲突

3. On the [Sender Address page](#), click **New**, configure the relevant parameters, and click **Submit** to complete the creation of a new sender address, which will be used as the sender address for emails sent by the Account Risk Control Platform.

**新建发信地址** ✕

发信域名  每个域名仅支持配置10个发信地址

邮箱前缀

发件人别名

发信地址预览

## Email template settings

1. On the [Send Mail Template page](#), click **New**, configure the relevant parameters, and click **Submit**. This template can then be used to invoke the email push service.

新建邮件模板
✕

模板名称 \*

模板类型 \* HTML富文本 纯文本

邮件摘要

邮件正文 \* 

点击上传 拖拽到此区域

请上传html文件

邮件内容中的变量使用{{变量名}}表示，如：尊敬的{{name}}

提交
预览
取消

| Parameter name     | ParameterDescription  | Parameter Templates  |
|--------------------|---|--|
| Template Name      | Custom Name.  | -  |
| Template type      | Choose according to actual needs. HTML Rich Text: Supports more styles and can present rich content. Plain Text: Only supports text.  | -  |
| Template Summary   | Custom Summary.   | -  |
| Email Message Body | Registration: When applying for a registration email template, the message body must contain and can only contain "otp" as a placeholder.   | [Tencent Security] Your email OTP is: {{ otp }}, and it is valid for 5 minutes. Please enter it promptly to avoid expiration.  |
|                    | Login: When applying for a login email template, the message body must contain and can only contain one placeholder, "otp".   | [Tencent Security] Your email OTP is: {{ otp }}, and it is valid for 5 minutes. Please enter it promptly to avoid expiration.  |
|                    | Two-Factor Authentication: When applying for a two-factor authentication email template, the message body must contain and can only contain one placeholder, "otp".               | [Tencent Security] Your email OTP is: {{ otp }}, and it is valid for 5 minutes. Please enter it promptly to avoid expiration.  |
|                    | Updating Email: In the template for requesting an email update, the message body must contain and can only contain one placeholder, "otp".  | [Tencent Security] Your email OTP is: {{ otp }}, and it is valid for 5 minutes. Please enter it promptly to avoid expiration.  |
|                    | Password Retrieval: In the email template for password retrieval requests, the body of the email must contain and can only contain two placeholders: "name" and "mailverifycode". | [Tencent Security] Dear {{ name }} user, you have initiated a password recovery through the "Forgot Password" function. Your verification code for this password recovery is: {{ mailverifycode }}. It is valid for 5 minutes. Please enter it promptly to avoid expiration. |
|                    | Retrieve Username: In the email template  | [Tencent Security] Dear user, you have retrieved   |

for retrieving usernames, the email body must contain and can only contain one placeholder, "name".

your username: {{ name }}.

2. On the Sending Template page, you can see the template that was just created. Copy the Sending Template ID.

| 模板id   | 模板名称   | 创建时间              | 当前状态 <span>①</span> | 操作                                    |
|--|--------|-------------------|---------------------|---------------------------------------|
| <span style="border: 1px solid red; padding: 2px;">[ID]</span> | [Name] | 2022/1/5下午5:41:42 | [Status]            | <a href="#">详情</a> <a href="#">删除</a> |

共 1 条 10 条 / 页

3. In the email template configuration of the Account Risk Control Platform, you need to fill in the titles and approved sender template IDs for seven emails: registration, login, two-factor authentication, email update, password recovery, and username recovery.

**Email service configuration** [Configuring an Email Template](#)

- Email service: Tencent Message Push
- Secret ID: [Redacted]
- SecretKey: [Redacted]
- Sender address: [Redacted]

**Email header template configuration**

- Registered Title: [Redacted]
- Registration Template: [Redacted]
 

When applying for a registered email template, the email body must contain and only contain one placeholder for otp. Reference template: [Tencent Security] Your email OTP is: {{ otp }}, and the valid time is: {{ time }}. Please enter as soon as possible to avoid invalidation.
- Login Title: [Redacted]
- Login Template: [Redacted]
 

When applying for a login email template, the email body must contain and only contain one placeholder for otp. Reference template: [Tencent Security] Your email OTP is: {{ otp }}, and the valid time is: {{ time }}. Please enter as soon as possible to avoid invalidation.
- Secondary Authentication Title: [Redacted]
- Secondary authentication template: [Redacted]
 

When applying for an email template for secondary authentication, the body of the email must contain and only contain one placeholder for otp. Reference template: [Tencent Security] Your email OTP is: {{ otp }}, and the valid time is: {{ time }}. Please enter as soon as possible to avoid invalidation.
- Update mailbox title: [Redacted]
- Update mailbox template: [Redacted]
 

When applying to update the mail template of the mailbox, the body of the mail must contain and can only contain a placeholder of otp. Reference template: [Tencent Security] Your email OTP is: {{ otp }}, and the valid time is: {{ time }}. Please enter as soon as possible to avoid invalidation.
- Retrieve password title: [Redacted]
- Retrieve password template: [Redacted]
 

When applying for an email template for recovering a password, the email body must contain and only contain two placeholders, name and malverifycode. Reference template: [Tencent Security] Dear {{ name }} user, hello: You initiate a password recovery through the "forgot password" function. The verification code for this password recovery is: {{ malverifycode }}, the effective time is: {{ time }}. Please enter as soon as possible to avoid invalidation.
- Retrieve username title: [Redacted]
- Retrieve username template: [Redacted]
 

In the username retrieving email template, name is the one and only placeholder in the message body. Sample: [Tencent Security] Dear user, you have retrieved your account: {{ name }}.

## Testing Email Service

1. After completing the input of the email template configuration information, before saving the email template configuration, you can click **Test Email Service Now** to test the email template configuration.

**Email service test**

Test now

OK

Cancel

2. In the Email Service Test box, enter a valid email address for testing, select the test template, and click **Send** to verify the

correctness of the configuration.

### Email service test ×

\* Email

\* Test template  Registration Template  Login Template

Secondary authentication template

Update mailbox template  Retrieve password template

Retrieve username template

3. After saving the email template configuration, you can test the email template configuration by clicking **Test Email Service Now** on the email template view interface.

# Identity verification template

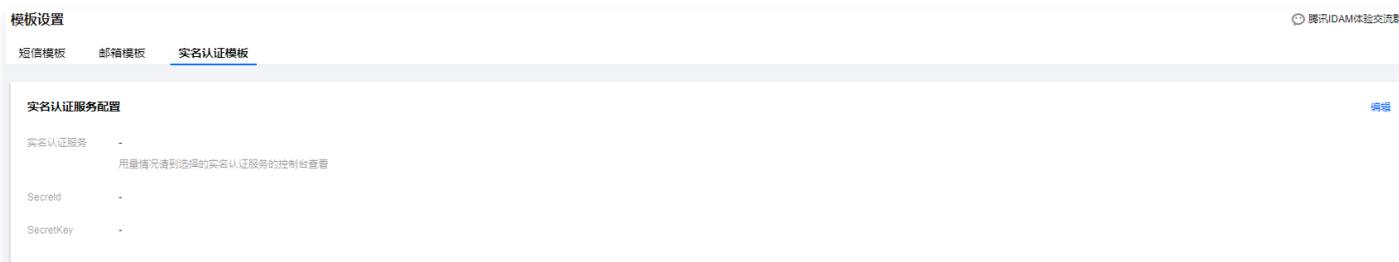
Last updated: 2023-09-04 10:39:32

## Scenario

The Account Risk Control platform supports the configuration of third-party identity verification services. After enabling identity verification during the application registration process, users can undergo identity verification when registering for the application.

## Configuring Identity Verification Template

1. Log in to the [Account Risk Control console](#). In the left sidebar, click **Personalized Settings > Template Settings > Identity Verification Template**.
2. On the Identity Verification Template page, if the current tenant has not configured an identity verification template, the system will display the following blank template information by default.



3. On the Identity Verification Template page, click **Edit** in the top-right corner of the interface.
4. On the editing page, select the identity verification service, enter the SecretId and SecretKey, and click **Confirm**.

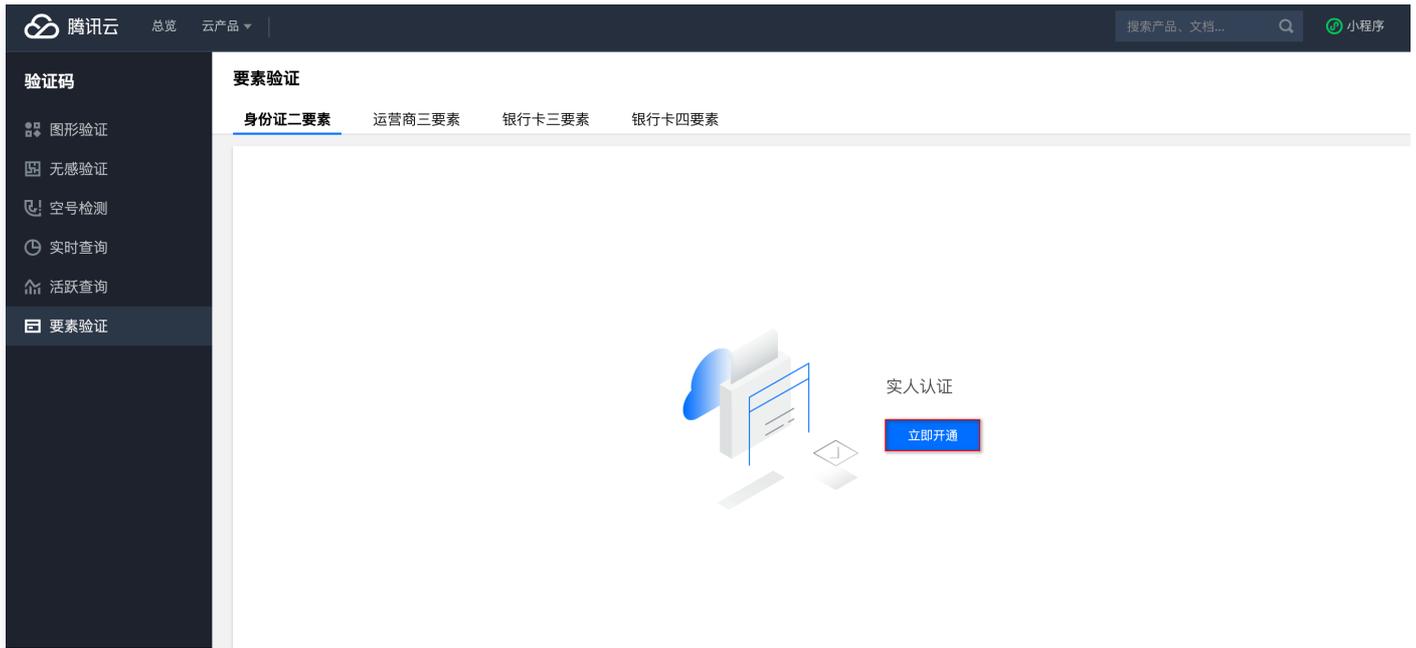
### Note

The identity verification service configuration supports various third-party identity verification services. By selecting a supported identity verification service, the page will dynamically load the configuration information required for that identity verification service.

## Activating the Skyeeye Identity Verification Service

1. Log in to the [CAPTCHA console](#) and click on **Element Verification** in the left sidebar.
2. Currently, the Account Risk Control platform supports two-factor (Name + ID number) and three-factor (Name + ID number + Mobile number) identity verification services. If tenants need to use these services, they can click **Activate Now** on the

corresponding page.



3. After successful activation, you can view usage data in the console after invoking the identity verification service.



## Obtaining the SecretId and SecretKey

1. Log in to the [Access Management Console](#). In the left sidebar, select **Users** > **User List** to navigate to the user list page.
2. On the User List page, select the desired sub-account and click on the **username** to enter the user details page.

### Note

If a sub-account is using Tencent Tianyu Identity Verification Service, you need to log in to the Access Management Console and authorize the sub-account with QcloudFIVFullAccess on the [Policy Page](#). For detailed operations, please refer to [Authorization Management](#).

| <input type="checkbox"/> 用户名称 | 用户类型 | 账号ID       | 创建时间       | 关联信息       | 操作                        |
|-------------------------------|------|------------|------------|------------|---------------------------|
| ▶ [Redacted]                  | 主账号  | [Redacted] | [Redacted] | [Redacted] | 授权 <a href="#">更多操作</a> ▼ |
| ▶ [Redacted]                  | 子用户  | [Redacted] | [Redacted] | [Redacted] | 授权 <a href="#">更多操作</a> ▼ |

3. On the User Details page, click **API Key**, select the required key, and click  to obtain the SecretId for this sub-account. Click **Show**, and after successful identity verification, you can obtain the SecretKey for this sub-account.

权限 服务 组 (0) 安全  **API 密钥** 小程序

 密钥最近访问时间为此密钥最近一次被调用的时间。

**新建密钥**

| 密钥  | 创建时间         | 最近访问时间     | 状态  | 操作 |
|---|--------------|------------|-----|----|
| SecretId: AI [Redacted]<br>SecretKey: *****  | 2 [Redacted] | 2021-06-15 | 已启用 | 禁用 |

## Utilizing Identity Verification Services

1. On the [Application Management page](#), select the application for which you want to configure the identity verification service, and click **Configure**.

应用管理 腾讯IDAM体验交流群

 平台提供创建Web、移动APP、小程序等类型应用，支持为应用配置个性化登录、注册、忘记密码、忘记用户名、MFA流程，支持自定义应用图标、域名等能力。

**新建应用** **删除**

| <input type="checkbox"/> | 应用名称/Client ID  | 应用类型  | 应用状态                                | 操作  |
|--------------------------|---|-------|-------------------------------------|---|
| <input type="checkbox"/> |  n. [Redacted]<br>YWZ [Redacted] | Web应用 | <input checked="" type="checkbox"/> |  <b>配置</b> <a href="#">体验</a> <a href="#">删除</a> |

共 1 条 10 条 / 页 

2. On the Application Configuration page, click **Process Configuration**, select the Registration Process module, and click **Edit**.

← **应用配置**

基本信息 **参数配置** 流程配置 安全域CORS

**注册流程** 

是否启用

认证属性 **电话号码**

普通属性 -

所属用户组 -

自动登录

实名认证

3. In the application process configuration, click on the  for identity verification to enable identity verification during the registration process and configure it.

### 注册流程

\* 是否启用

\* 认证属性

普通属性

所属用户组

自动登录

实名认证

#### 📌 Note

- **Verification Method:** Choose the identity verification method for the registration process, including two-factor verification (name + ID number) and three-factor verification (name + ID number + phone number). The prerequisite for the verification method to take effect is that the [Identity Verification Service Configuration](#) has been completed in the template settings, and the properties in the registration process include the fields required for identity verification.
- **Registration Result:** The impact of the identity verification result on the registration process, including two methods: registration continues despite verification failure, and registration is halted upon verification failure.

# Image CAPTCHA

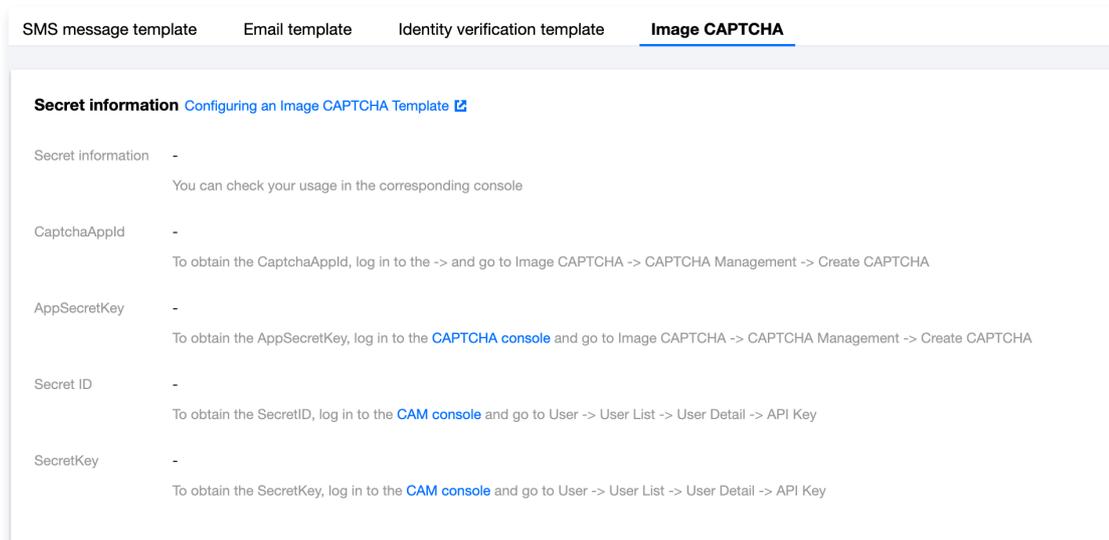
Last updated: 2023-09-04 10:39:38

## Scenario

The risk control platform by default provides each tenant with 200 free image verification codes. Once this free quota is exceeded, the platform will suspend the sending of image verification codes to the tenant, affecting portal registration, SMS OTP authentication source login, and MFA secondary authentication. To ensure the normal operation of the business, administrators need to configure the CAPTCHA service to provide image verification code services for platform operations.

## Configure Image Verification Code Template

1. Log in to the [Account Risk Control Platform console](#), and select **Personalized Settings > Template Settings > Image Verification Code Template** from the left sidebar.
2. On the Image Verification Code Template page, if the current tenant has not configured an image verification code template, the system will display the following blank template information by default.



3. On the Image Verification Code Template page, click **Edit** in the top-right corner.
4. On the editing page, select **Image Verification Code Service**, enter **CaptchaAppId**, **AppSecretKey**, **SecretId**, and **SecretKey**, then click **Confirm**.

### Note

Different image verification code services require different parameters. Currently, the platform only supports the **Tencent Tianyu** image verification code service, and will gradually support the configuration of other image verification code services. The following are the relevant parameters needed to configure the Tencent Tianyu image verification code service.

**Secret information** [Configuring an Image CAPTCHA Template](#)

• Secret information   
You can check your usage in the corresponding console

• CaptchaAppId   
To obtain the CaptchaAppId, log in to the -> and go to Image CAPTCHA -> CAPTCHA Management -> Create CAPTCHA

• AppSecretKey   
To obtain the AppSecretKey, log in to the [CAPTCHA console](#) and go to Image CAPTCHA -> CAPTCHA Management -> Create CAPTCHA

• Secret ID   
To obtain the SecretID, log in to the [CAM console](#) and go to User -> User List -> User Detail -> API Key

• SecretKey   
To obtain the SecretKey, log in to the [CAM console](#) and go to User -> User List -> User Detail -> API Key

## Image Verification Service Configuration

### Obtain CaptchaAppId and AppSecretKey

#### Note

To obtain the CaptchaAppId and AppSecretKey, you must first purchase the [CAPTCHA Package](#).

1. Log in to the [CAPTCHA console](#), and select **Image Verification > Verification Management** from the left sidebar.
2. On the Verification Management page, click **Create Verification**.

#### 图形验证

[验证管理](#)[验证统计](#)[套餐包管理](#)[新建验证](#)[快速接入](#)

3. In the new verification pop-up window, set parameters such as verification name, client type, and verification method according to business scenario requirements, and click **Confirm** to complete the creation of the authentication.

4. Upon completion of the new verification, you can view the `CaptchaAppId` and `AppSecretKey` on the Verification Management page.

## Obtaining the SecretId and SecretKey

1. Log in to the [Access Management Console](#), and select **Users > User List** from the left sidebar.
2. On the User List page, select the required **sub-account**, click on the **username** to enter the user details page.

| 用户名称 | 用户类型 | 账号ID | 创建时间 | 关联信息 | 操作      |
|------|------|------|------|------|---------|
| 主账号  | 主账号  |      |      |      | 授权 更多操作 |
| 子用户  | 子用户  |      |      |      | 授权 更多操作 |

3. On the User Details page, click **API Key**, select the required key, and click to obtain the SecretId for this sub-account; click

Show, and after successful identity verification, you can obtain the SecretKey for this sub-account.

权限 服务 组 (0) 安全 ⓘ API 密钥 小程序

ⓘ 密钥最近访问时间为此密钥最近一次被调用的时间。

新建密钥

| 密钥   | 创建时间 | 最近访问时间     | 状态  | 操作 |
|--|------|------------|-----|----|
| SecretId: AI<br>SecretKey: ***** <span>显示</span> | 2    | 2021-06-15 | 已启用 | 禁用 |