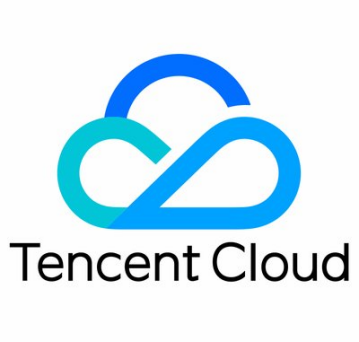
Customer Identity Access Management Operation Guide



Contents

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

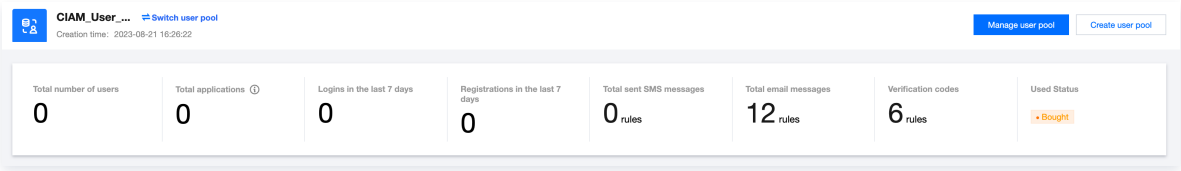
Last updated: 2023-09-04 10:29:49

Scenario

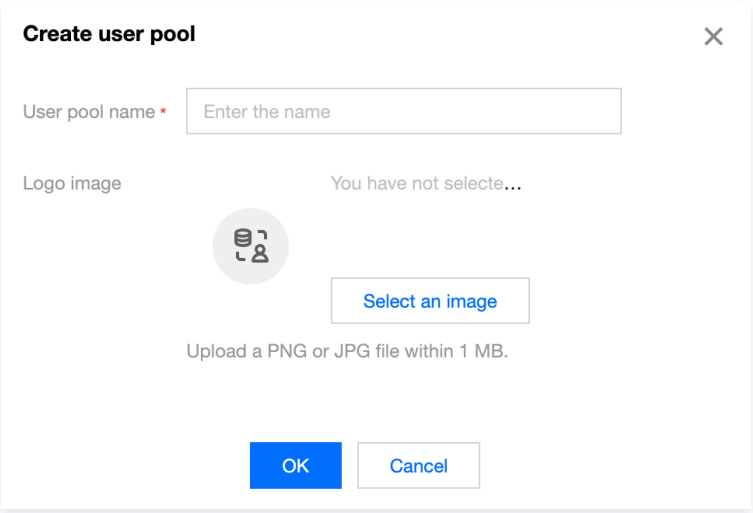
The user pool serves as the primary directory in the Account Risk Control platform, isolating all user data, custom attribute data, application data, and authentication source data. Before using the Account Risk Control platform for the first time, you need to create a user pool. The platform supports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



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

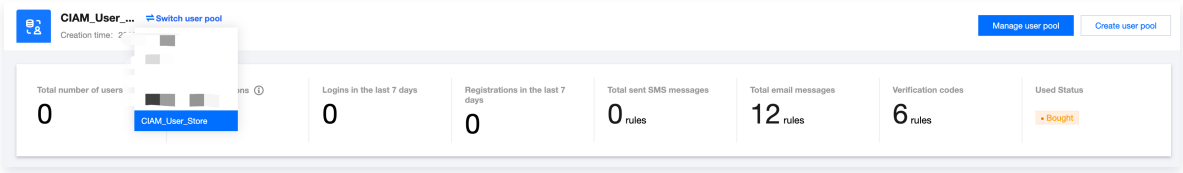
Last updated: 2023-09-04 10:29:56

Scenario

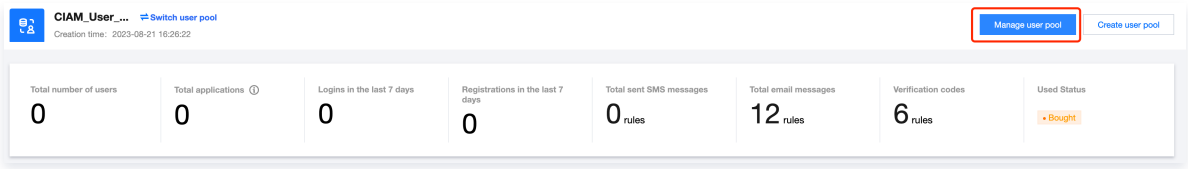
The Account Risk Control Platform supports multiple user directories. If an administrator needs to manage and configure different user directories, this can be accomplished by switching between user directories.

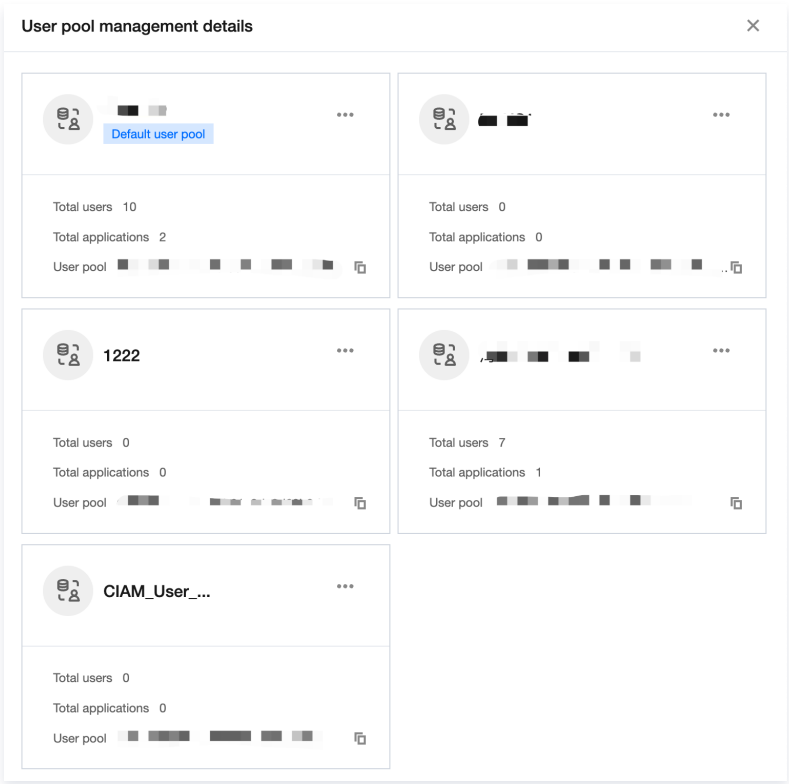
Instructions

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

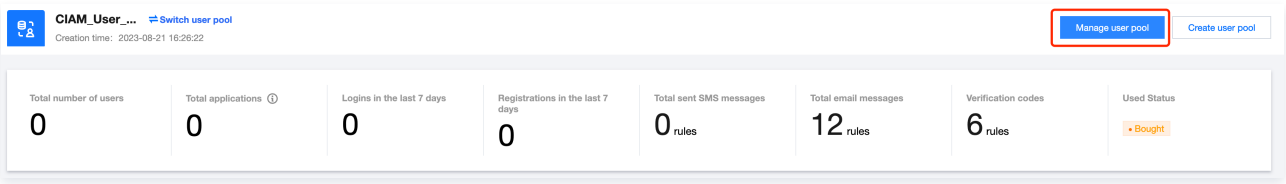
Last updated: 2023-09-04 10:31:50

Scenario

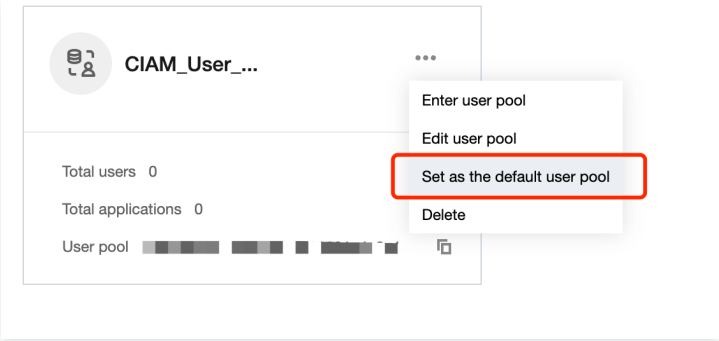
The Account Risk Control Platform supports multiple user directories. If an administrator has a user directory that needs to be managed as a priority, this can be accomplished by setting a default user directory. Once set, the administrator will automatically enter the designated user directory upon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

Instructions

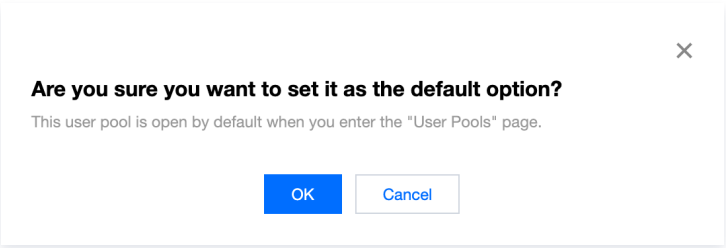
1. Log in to the Account Risk Control Platform Console, select **Overview** from the left sidebar to navigate to the Overview page.
2. On the Overview page, click on **Manage User Directory** at the top right of the interface to enter the User Directory Management Details page.



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

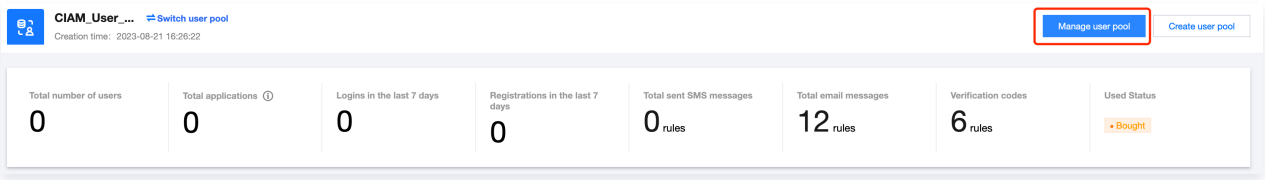
Last updated: 2023-09-04 10:31:57

Scenario

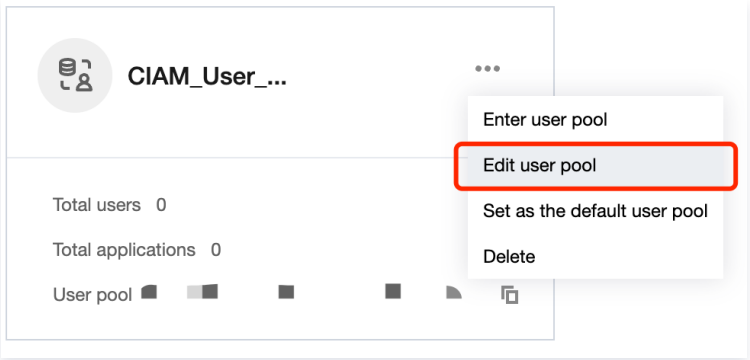
Upon successful creation of the user directory, you can modify the user directory information, such as the user directory name, Logo image, and so on.

Instructions

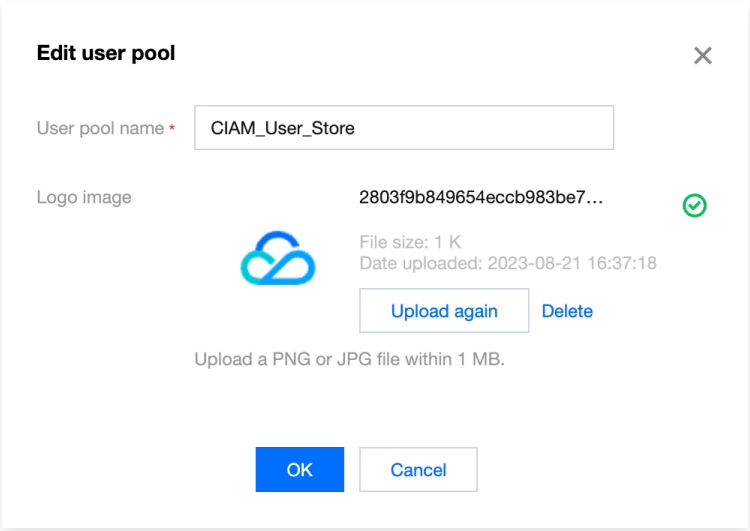
1. Log in to the Account Risk Control Platform Console, select **Overview** from the left sidebar to navigate to the Overview page.
2. On the Overview page, click on **Manage User Directory** at the top right of the interface to enter the User Directory Management Details page.



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.

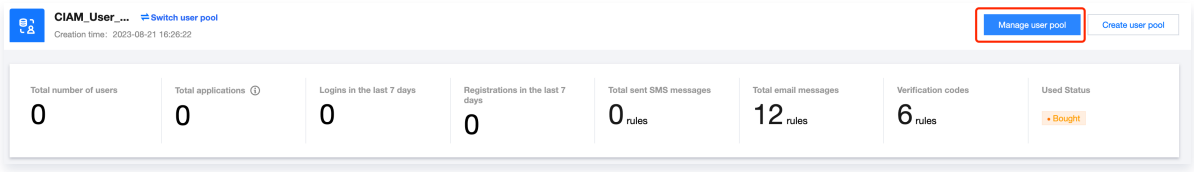
> **Note**
> Deleting a user directory will erase all data within it, including users, custom attributes, user groups, applications, authentication sources, and all other information. Please proceed with caution.

Preparations

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

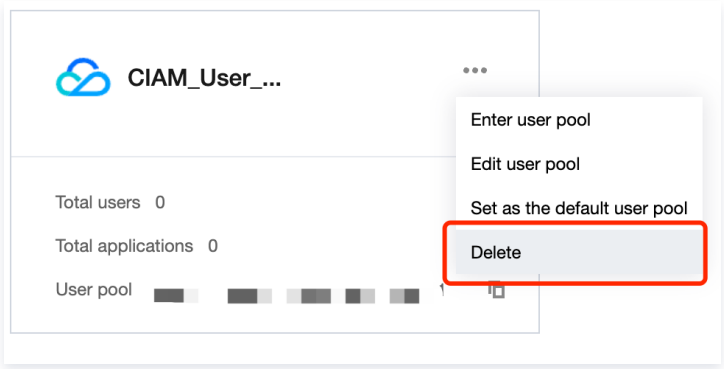
Instructions

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.

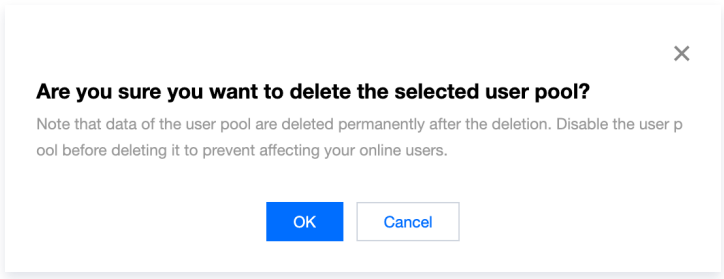


3. On the User Directory Management Details page, click ••• , then select **Delete**.

> **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

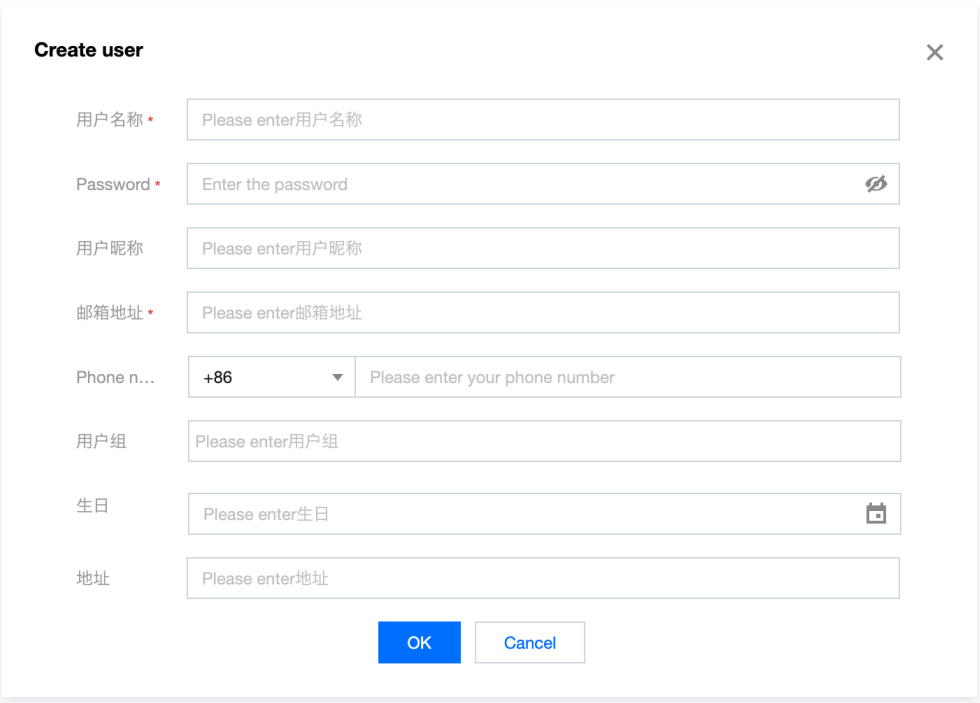
Scenario

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.



Viewing user details

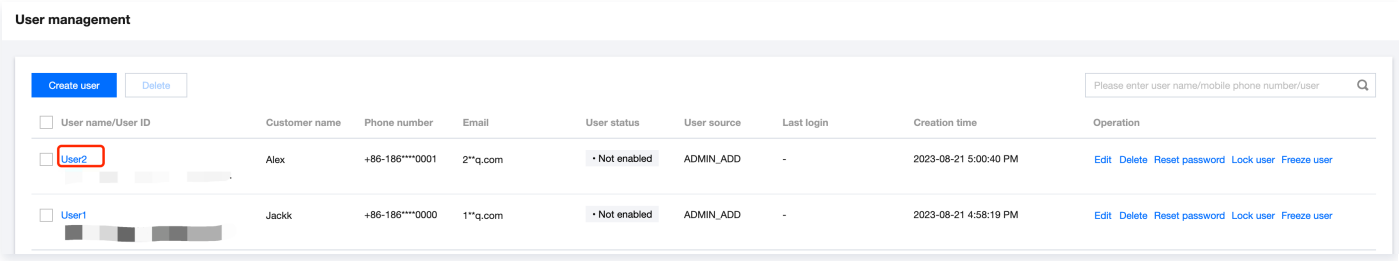
Last updated：2023-09-04 10:32:16

Scenario

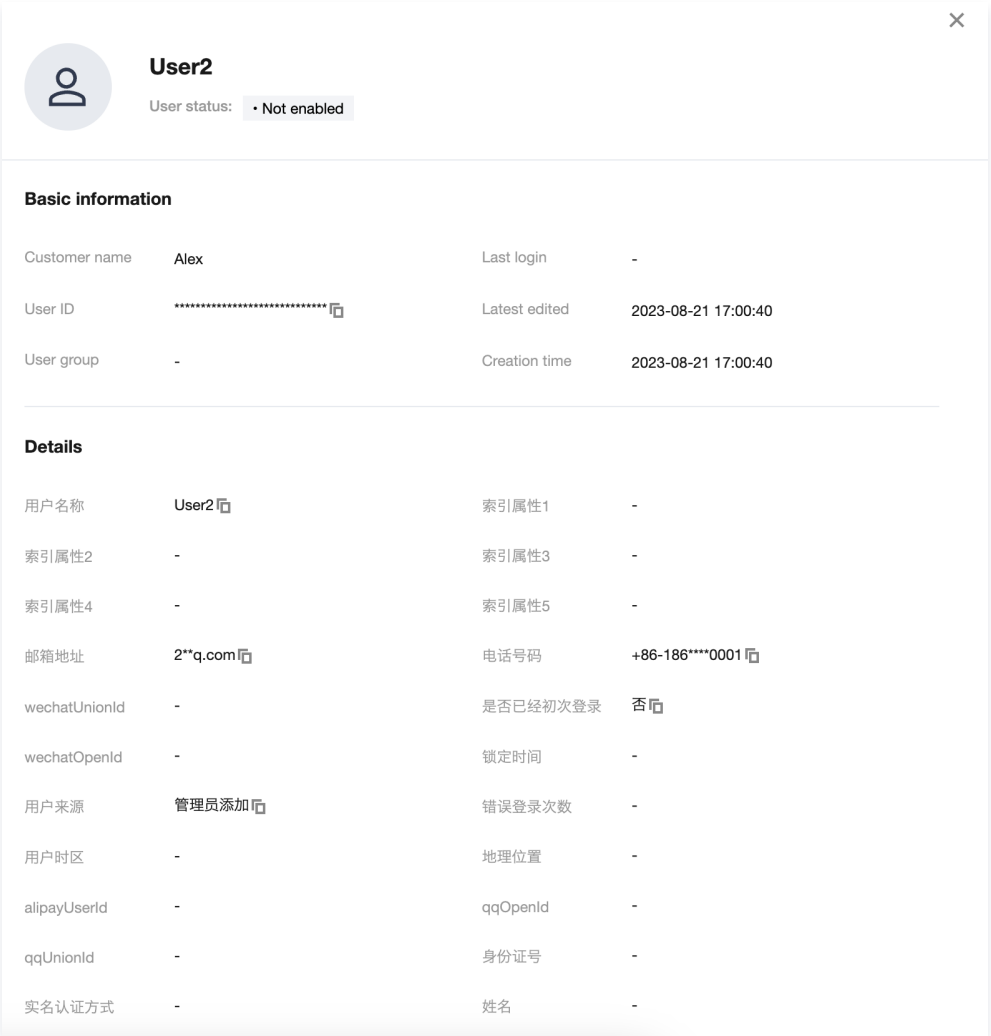
Upon successful addition of a user, you can view detailed user information, such as basic details and affiliated user groups.

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

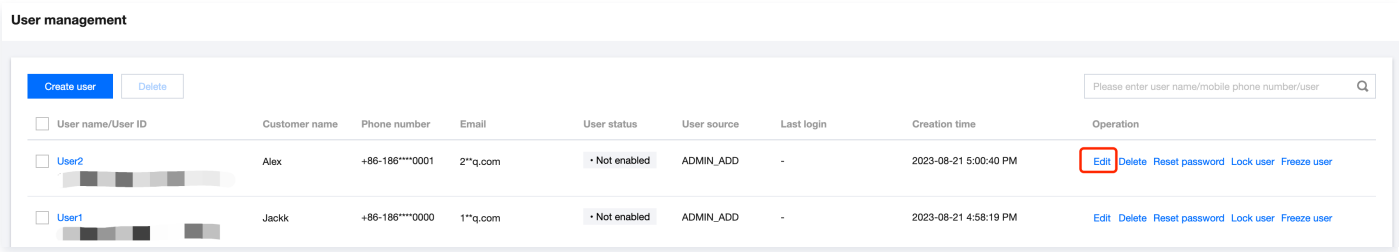
Last updated: 2023-09-04 10:32:21

Scenario

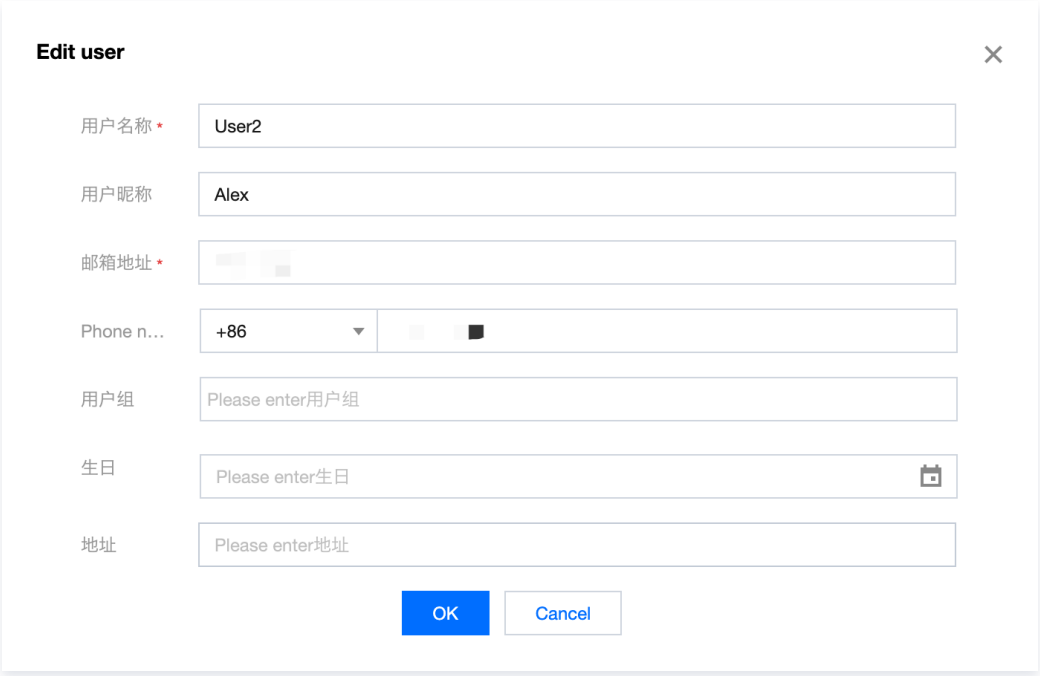
Upon successful addition of a user, it is possible to modify user attribute information such as the user name, associated email, and phone number.

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.



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



Deleting a user

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

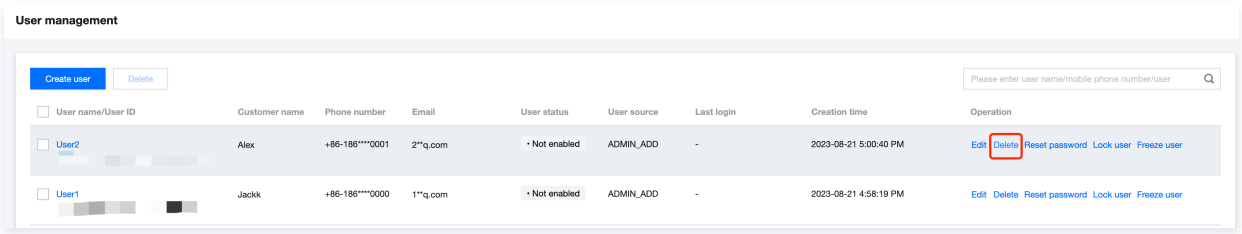
Scenario

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

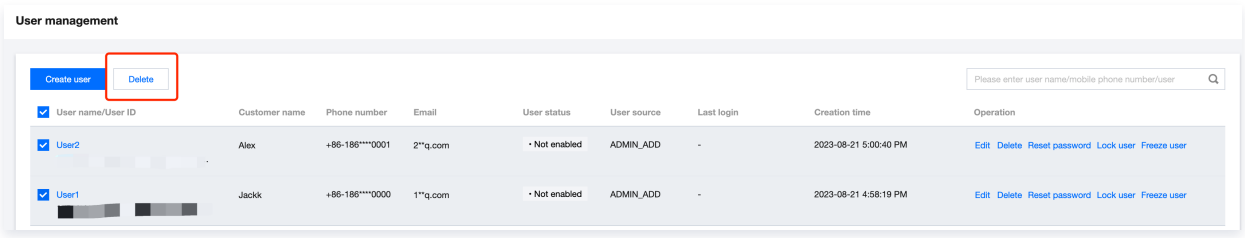
> **Note**
> Note that after the deletion, all data will be cleared and cannot be restored.

Instructions

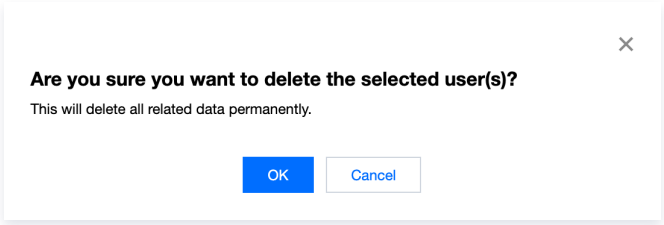
1. Log in to the Account Risk Control Console, and from the left navigation bar, select **User Management** > **User Management**.
2. On the User Management page, you have the option to delete individual or multiple users.
   - To delete a single user: Select the user you wish to remove, then click on **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

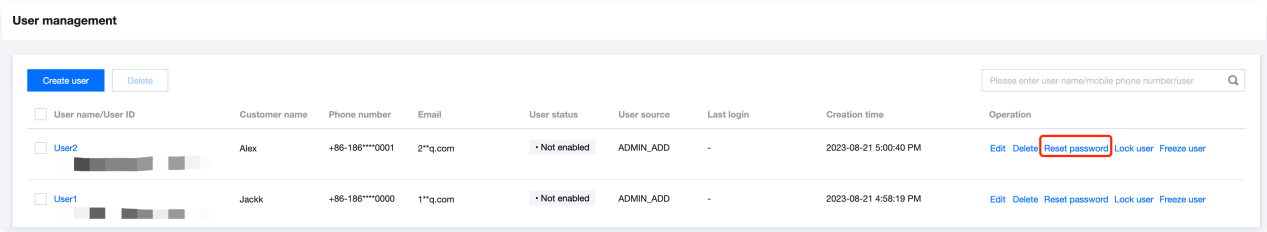
Last updated: 2023-09-04 11:19:40

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.

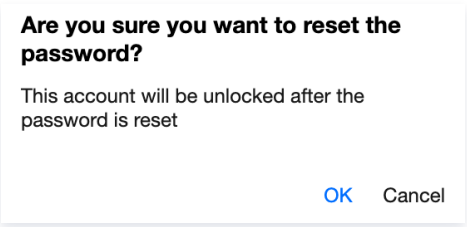
Instructions

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.



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

> **Note**
> Resetting the password will unlock the account.



Freezing or locking users

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

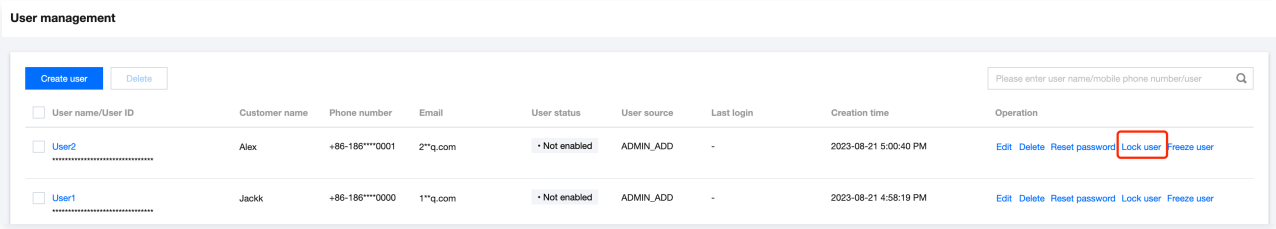
Scenario

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

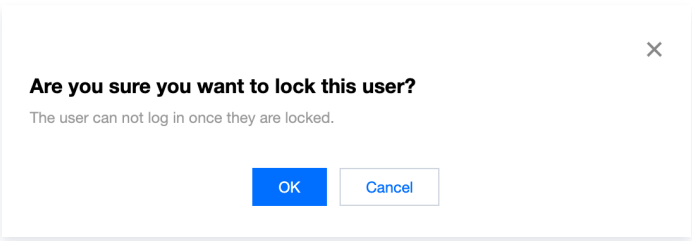
Locking a User

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.



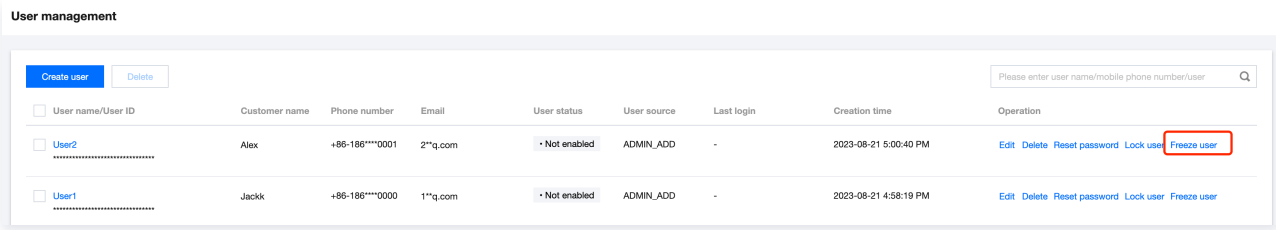
3. In the "Confirm Lock" pop-up window, click **OK**. The user will then be locked and unable to log in to the console.

> **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.

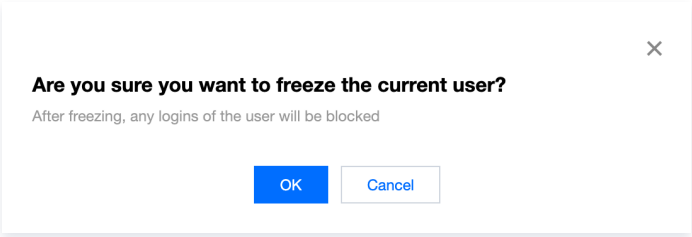


Freeze user

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.



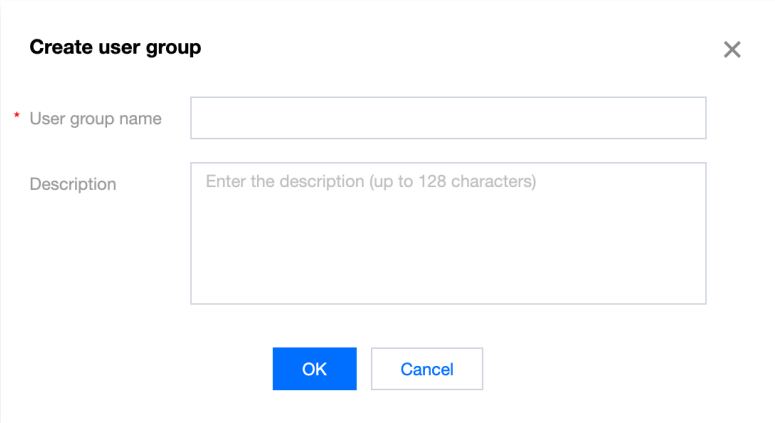
User group management

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.



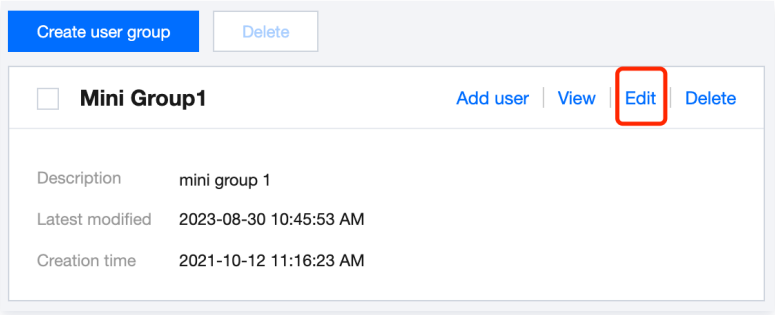
Parameter Description:

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

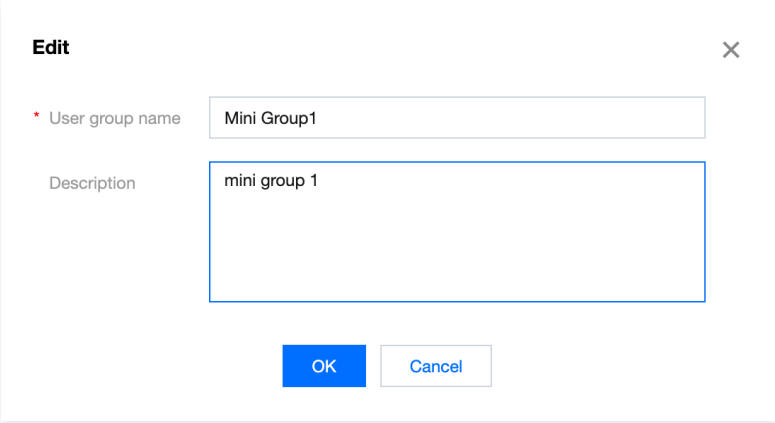
Edit User Group

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.



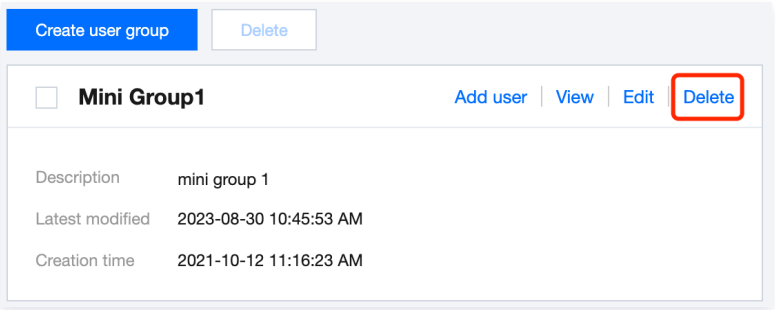
2. In the edit pop-up window, modify the user group name and notes, then click **OK** to confirm.



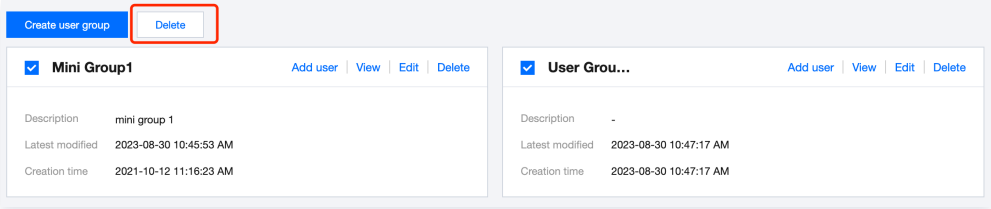
Delete user group

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.



- 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

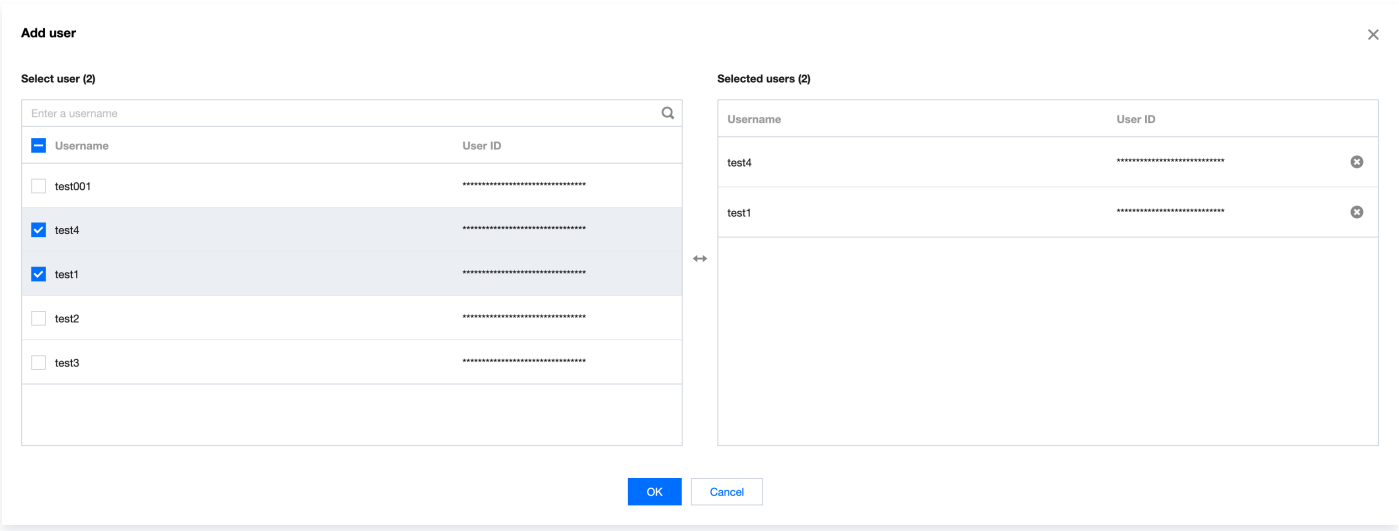


Adding users to the user group

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

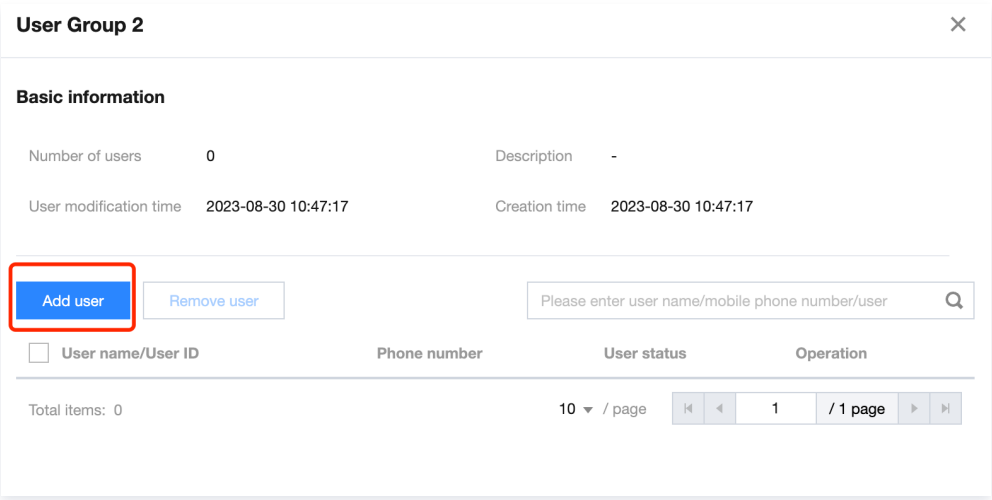
Method 1

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.

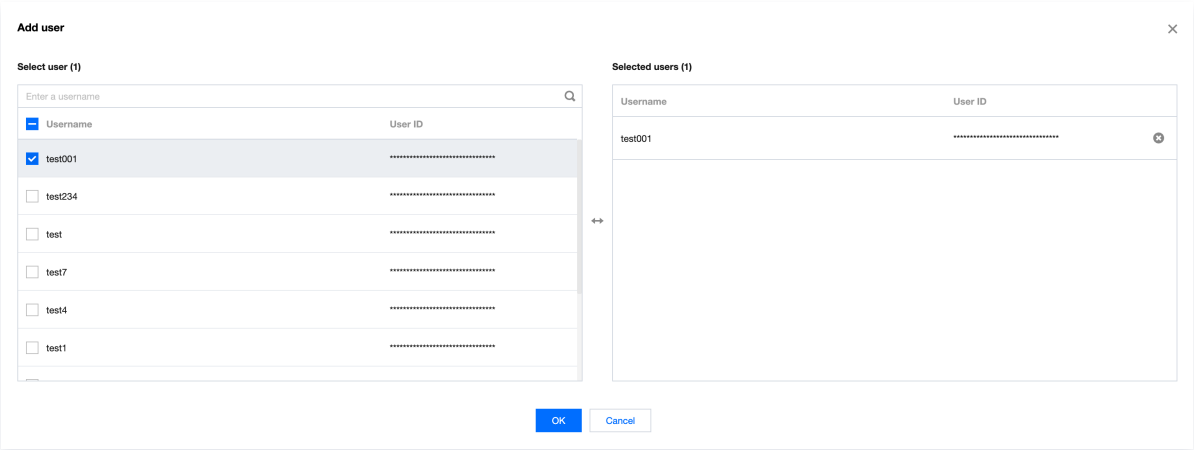


Method 2

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.

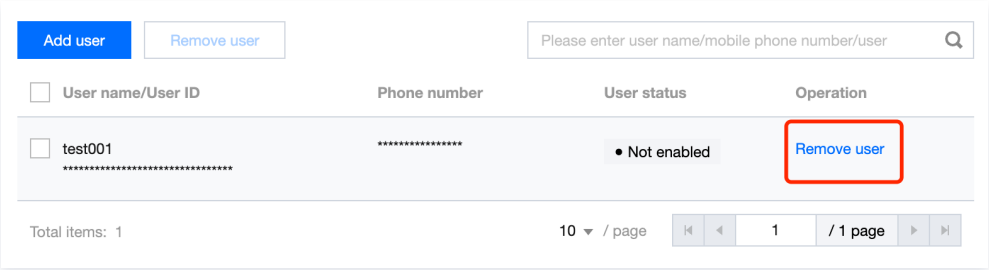


Remove user from user group

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

Method 1

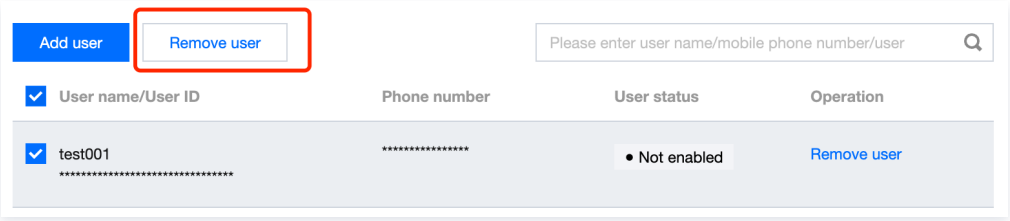
1. On the User Group Management page, select the desired user group and click on its blank area to enter the User Group Details page.
2. On the User Group Details page, click **Remove User** in the operation column on the right.



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

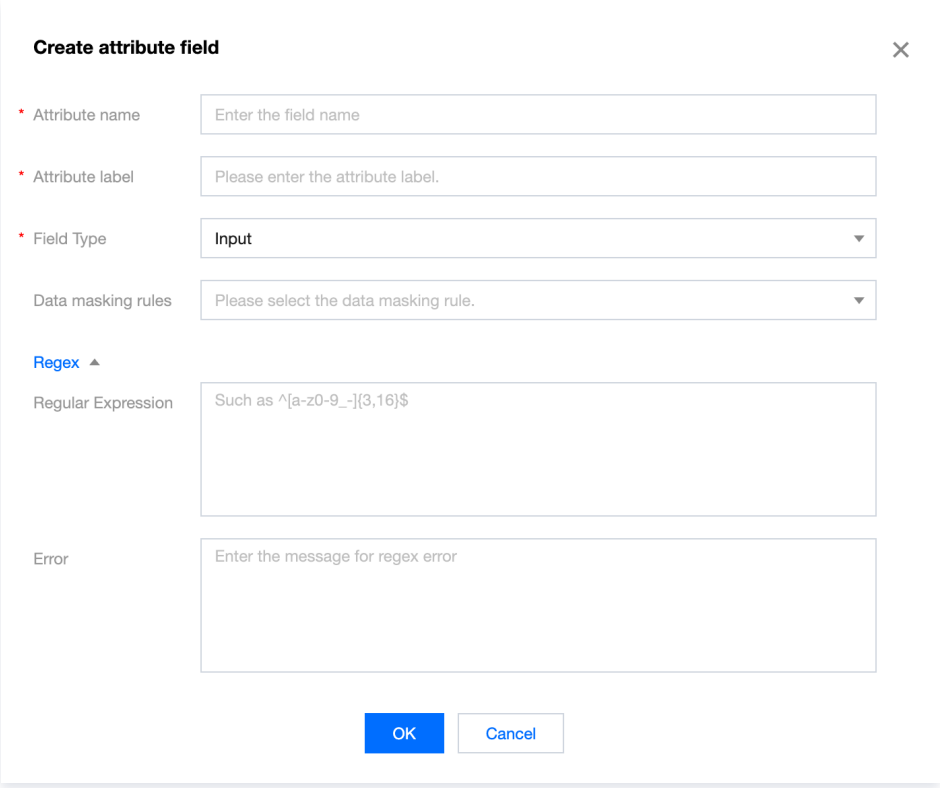
Scenario

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.



Editing a custom attribute

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

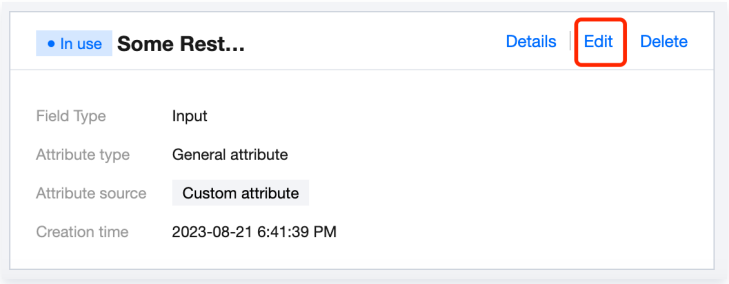
Operational Overview

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

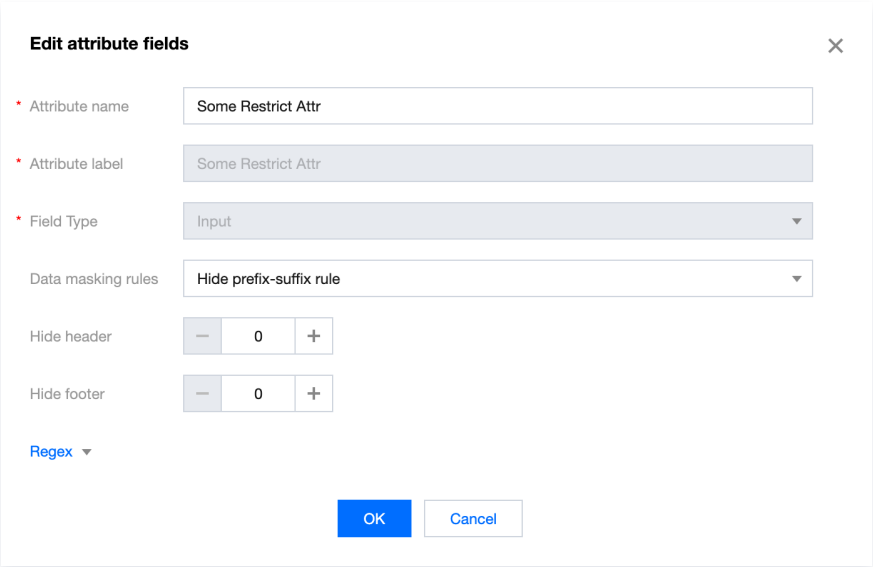
> **Note**
> Inbuilt attributes cannot be edited, while preset and custom attributes are editable.

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**.



Viewing custom attributes

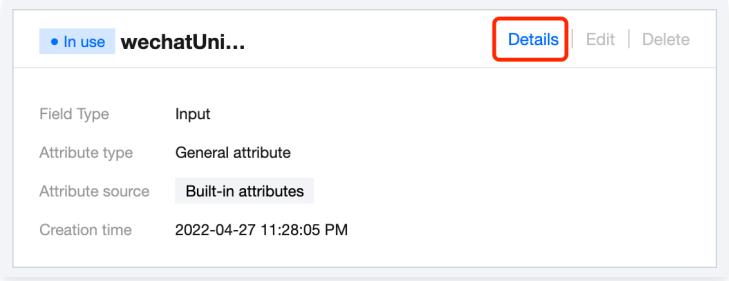
Last updated: 2023-09-04 10:33:02

Scenario

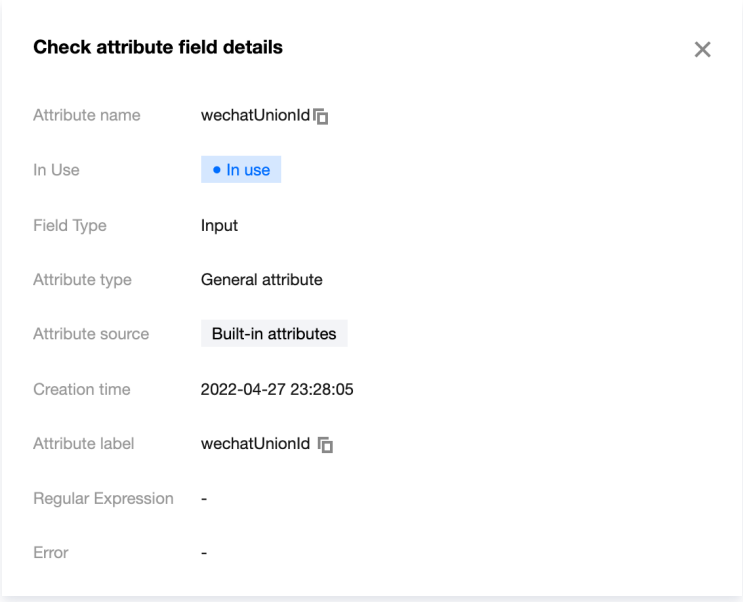
Upon successful addition of a custom attribute, one can view details such as attribute fields, regular expressions, and error prompts.

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

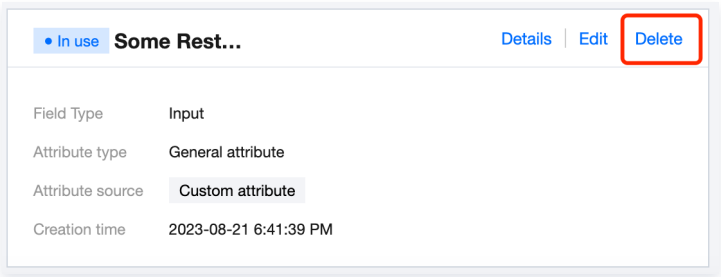
Scenario

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.

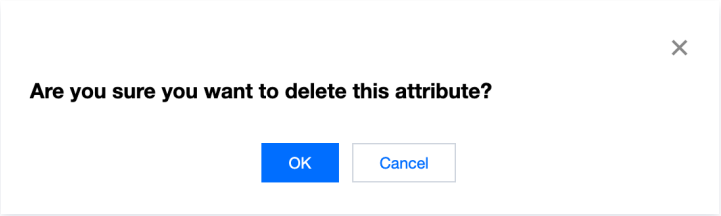
Instructions

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

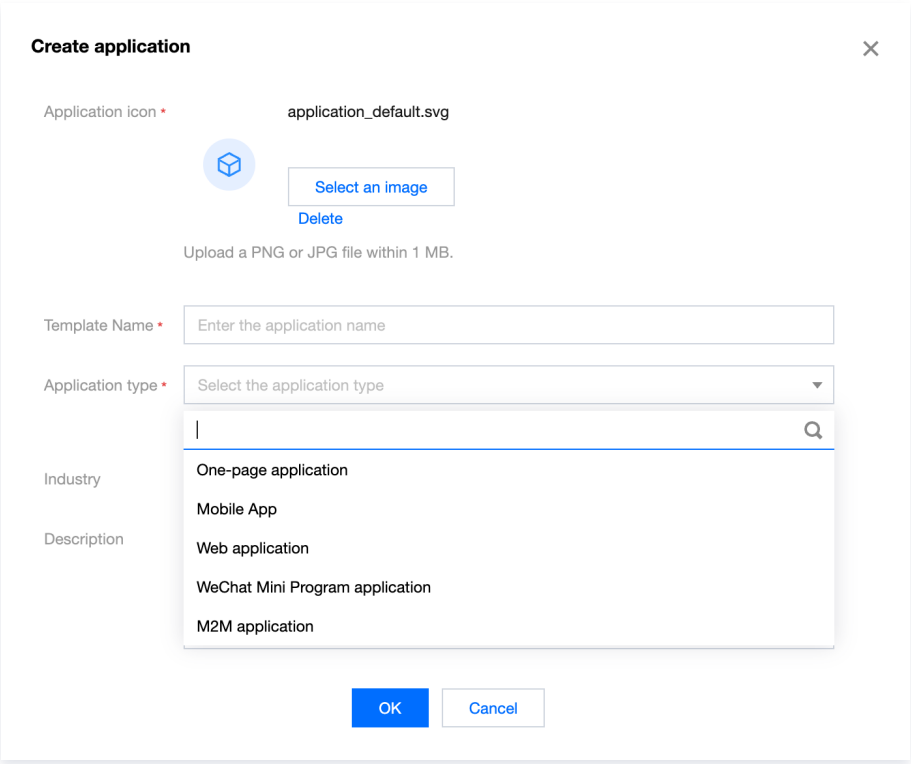
Scenario

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.



App Configuration

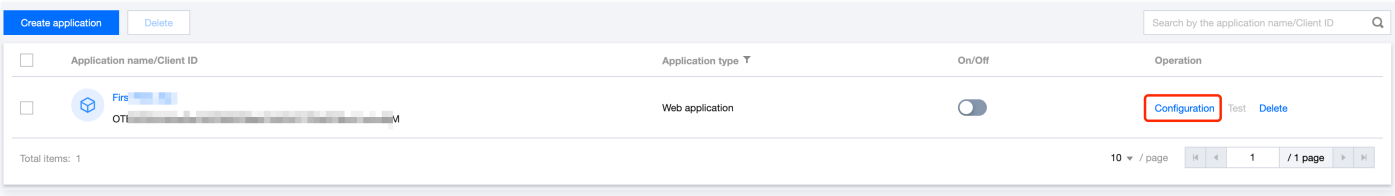
Last updated: 2023-09-04 11:28:24

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).

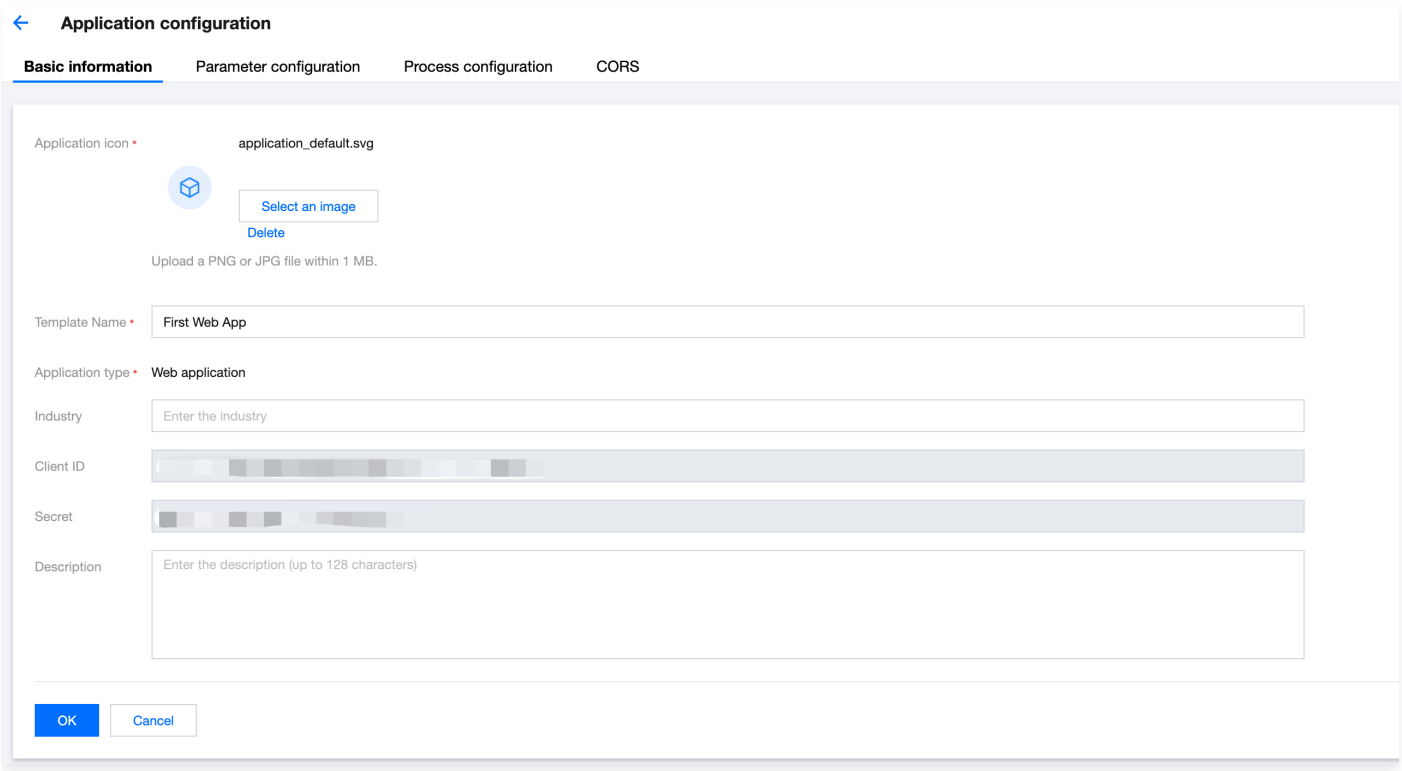
Instructions

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.



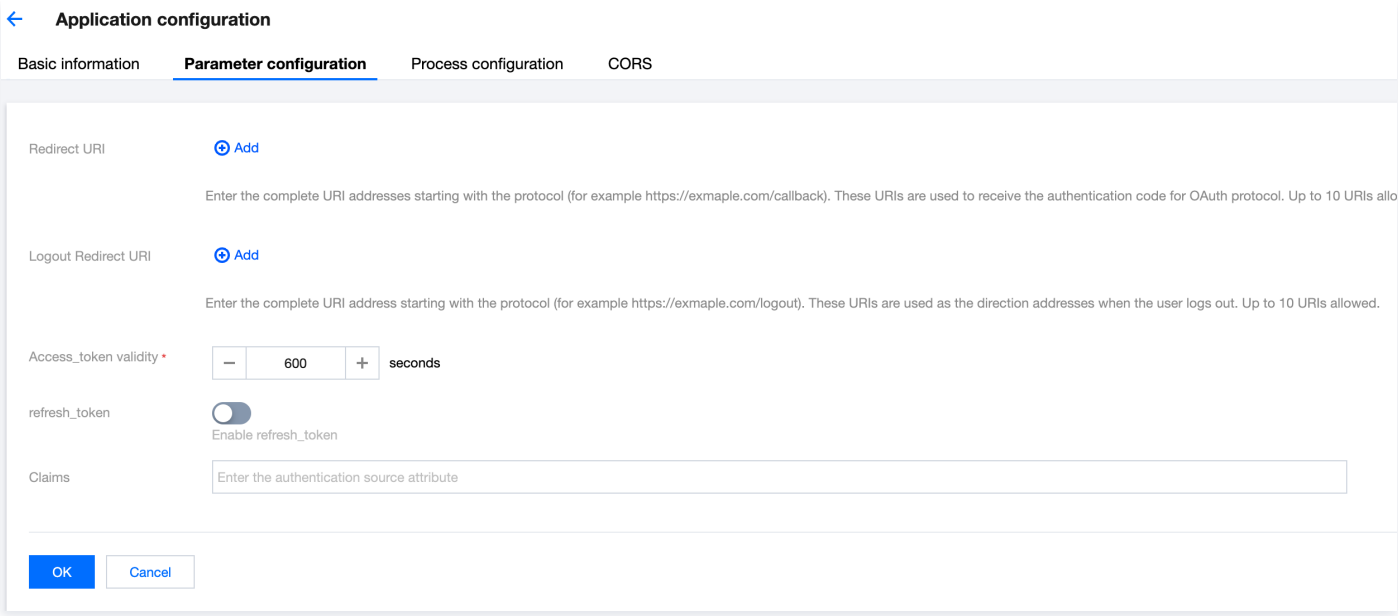
Basic information

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



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.



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.	https://www.qq.com
Logout Redirect URI	Enter a complete URL starting with http or https, which will serve as the redirect address after the user logs out.	https://www.qq.com/logout
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

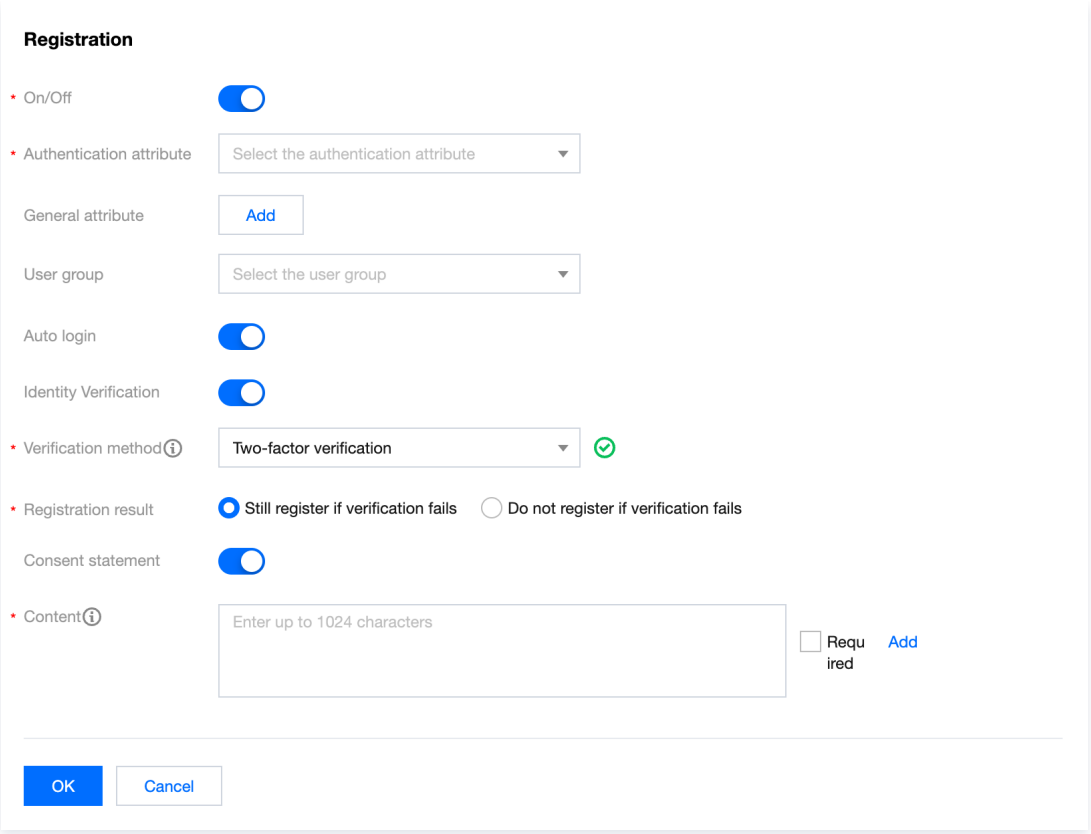
Process Configuration

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

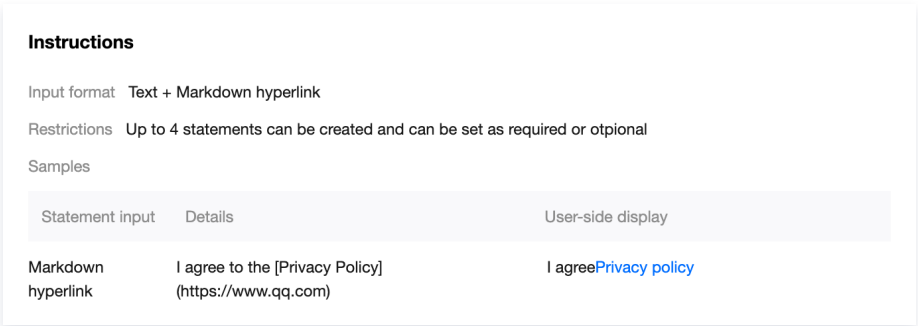
1. On the Application Configuration page, click **Parameter Settings** to switch to the parameter configuration page for process configuration.
2. The Parameter Configuration page includes five major modules: Registration Process, Login Process, MFA Process, Forgotten Username Process, and Forgotten 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.

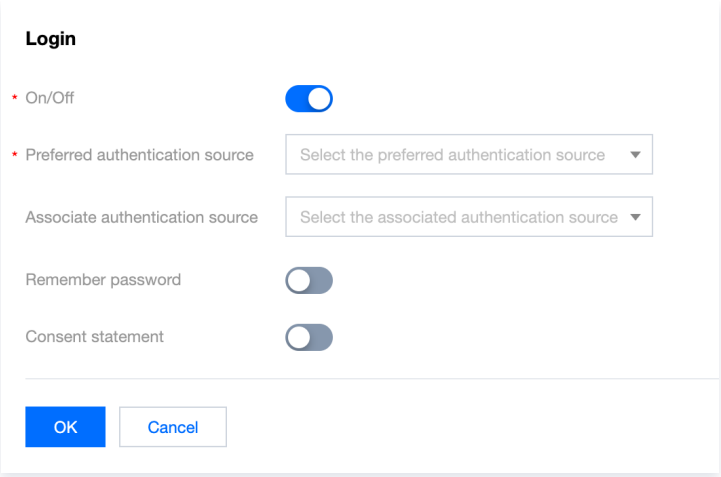


Parameter Description:

- 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.

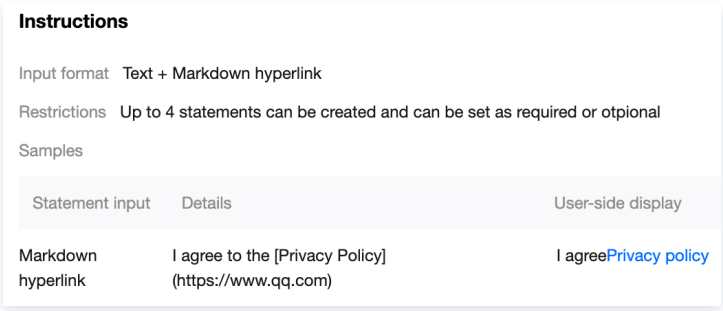


- **Login Process**: Click **Edit** in the upper right corner of the module, configure the relevant parameters, and click **OK** to save the configuration.

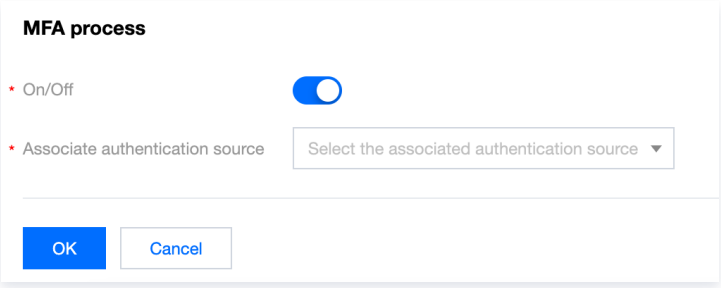


Parameter Description:

- 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.



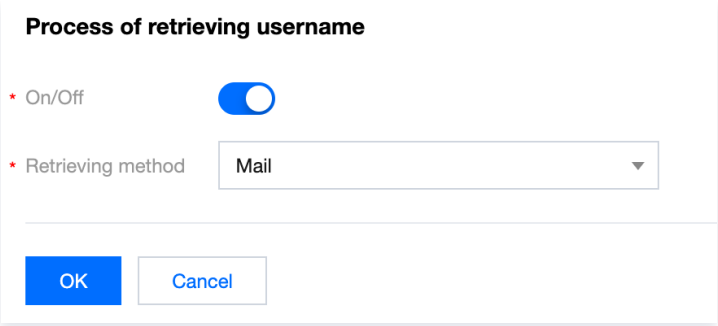
- **MFA Process**: Click **Edit** in the upper right corner of the module, configure the relevant parameters, and click **OK** to save the configuration.



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.

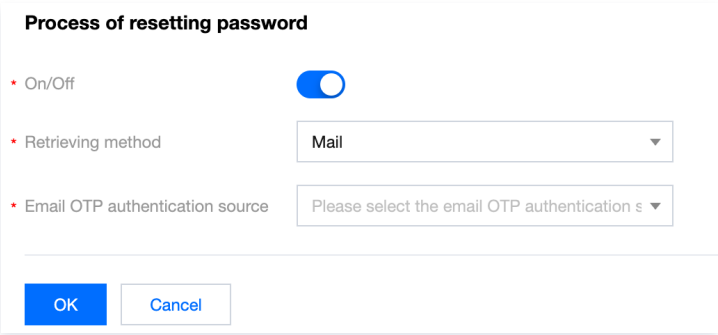
- **Process of Retrieving Username**: Click **Edit** in the upper right corner of the module, configure the relevant parameters, and click **OK** to save the configuration.



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.

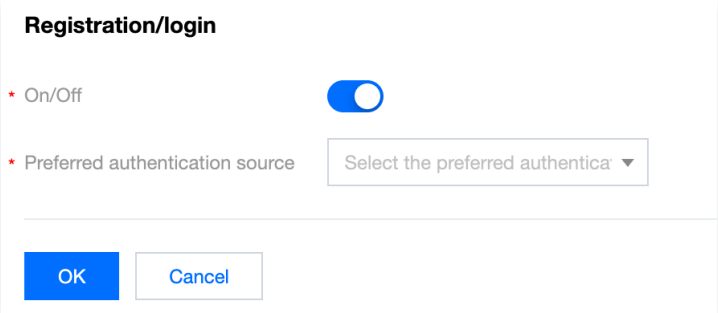


Parameter Description:

- 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.



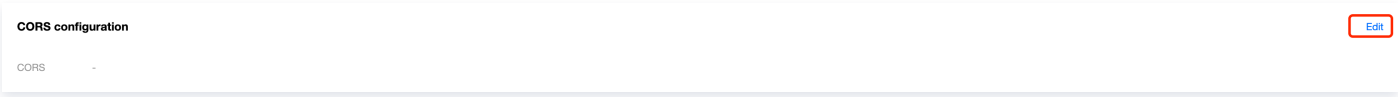
Parameter Description:

- 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.

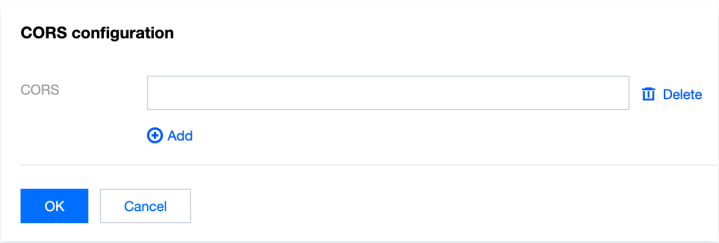
Security Domain CORS

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.

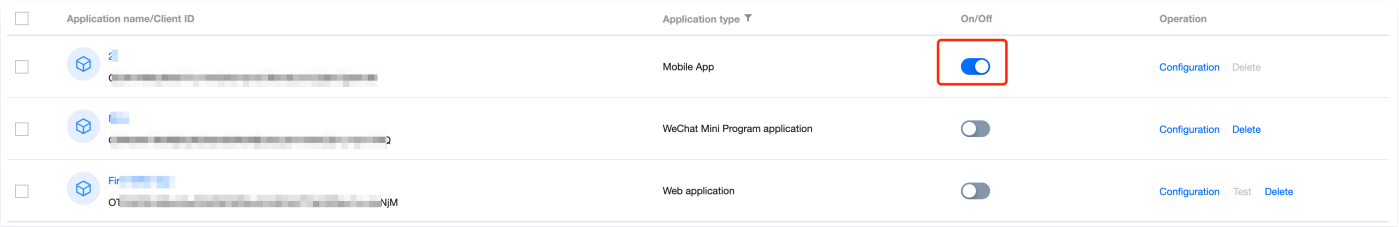
Instructions

Experience Web, Single Page, and Mobile App Applications

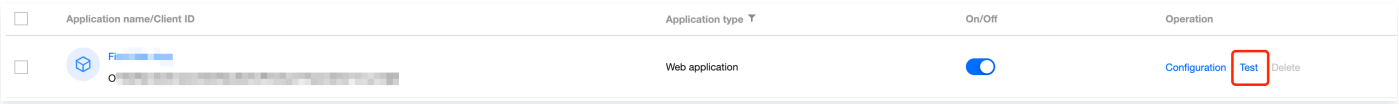
For Web applications, single-page applications, and mobile apps, you can quickly experience the effects of the configuration once the application is enabled.

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.



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

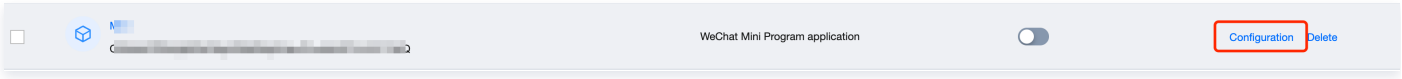


4. On the Demo demonstration page, you can swiftly experience the application's registration, login, and other functions. After a successful login, you will be redirected to the following Demo page.

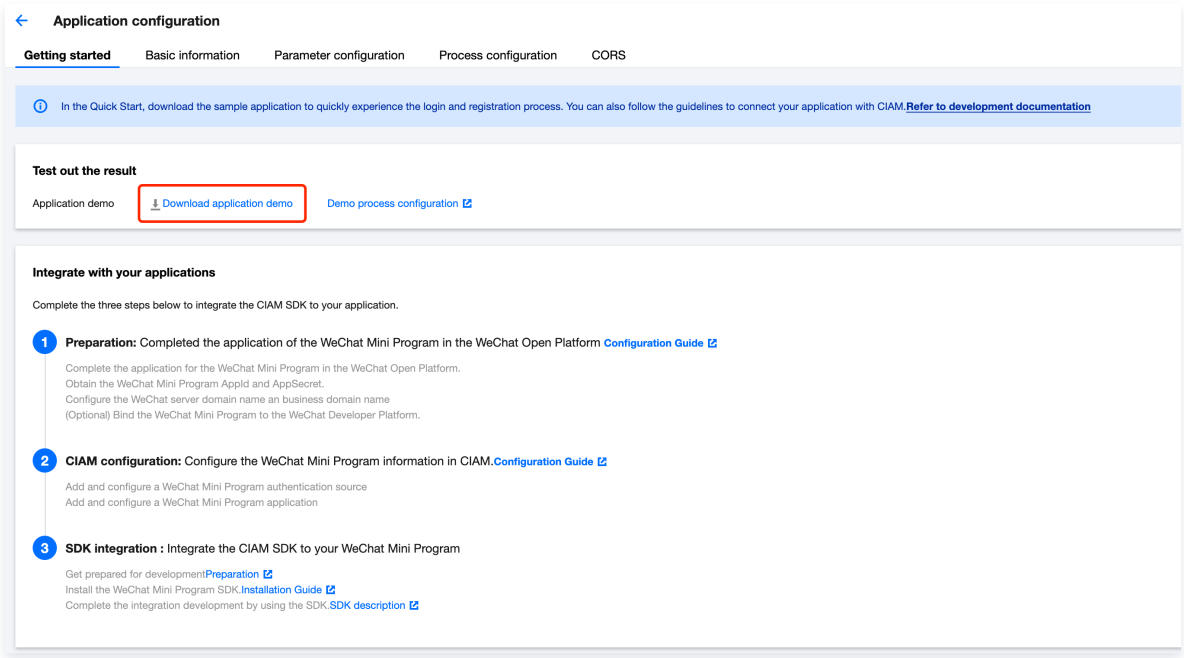
Experience Mini Program Applications

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.



Authentication management
General authentication sources
Creating an authentication source
Account and Password Authentication

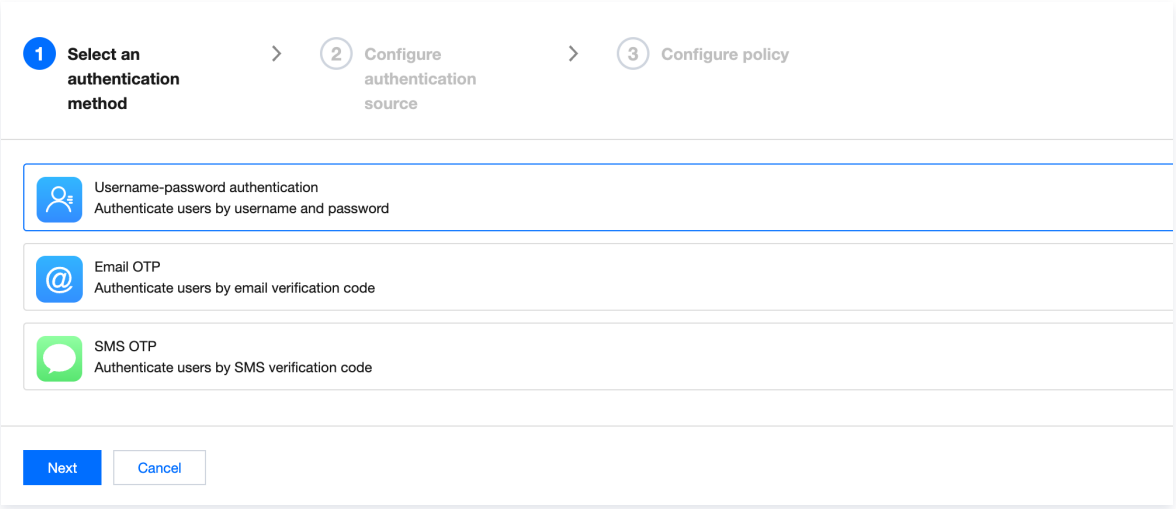
Last updated: 2023-09-04 11:40:19

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.

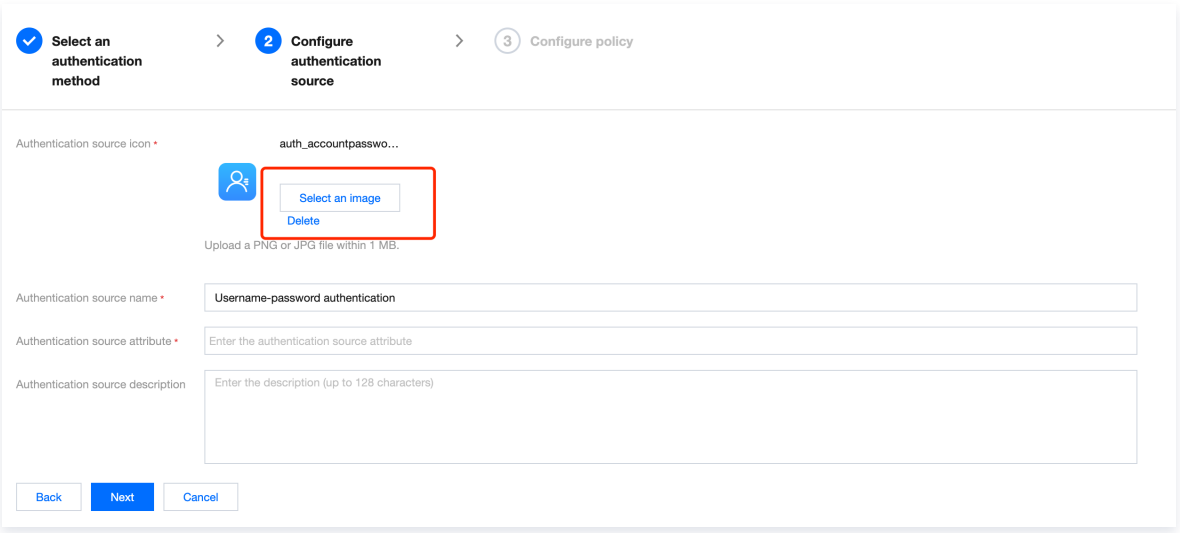
Instructions

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**.

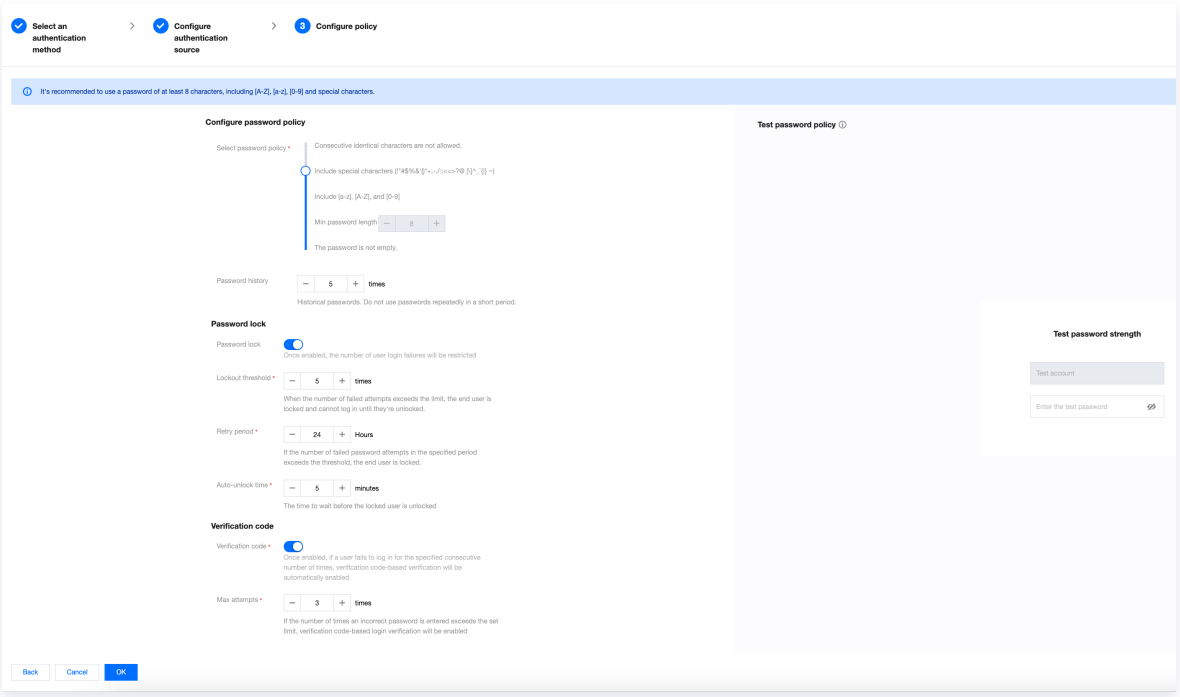


4. On the Create Authentication Source page, set the authentication source icon, name, attributes, and description, then click **Next**.

> **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.



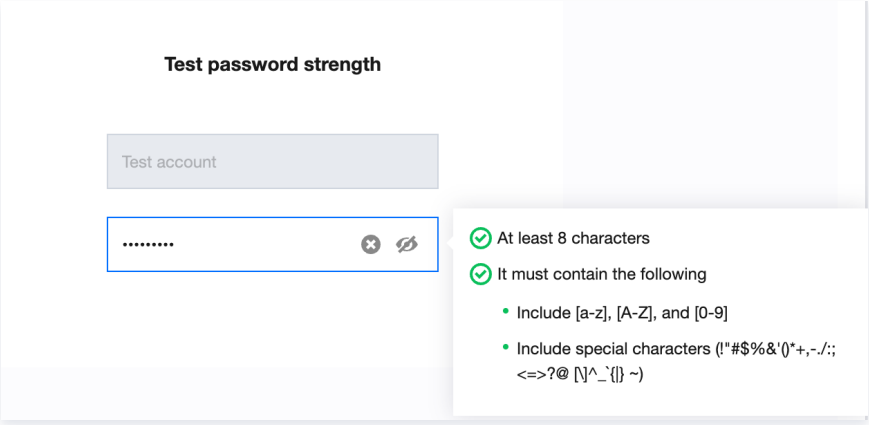
Configure Policy Parameter Notes

- **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.



SMS OTP

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

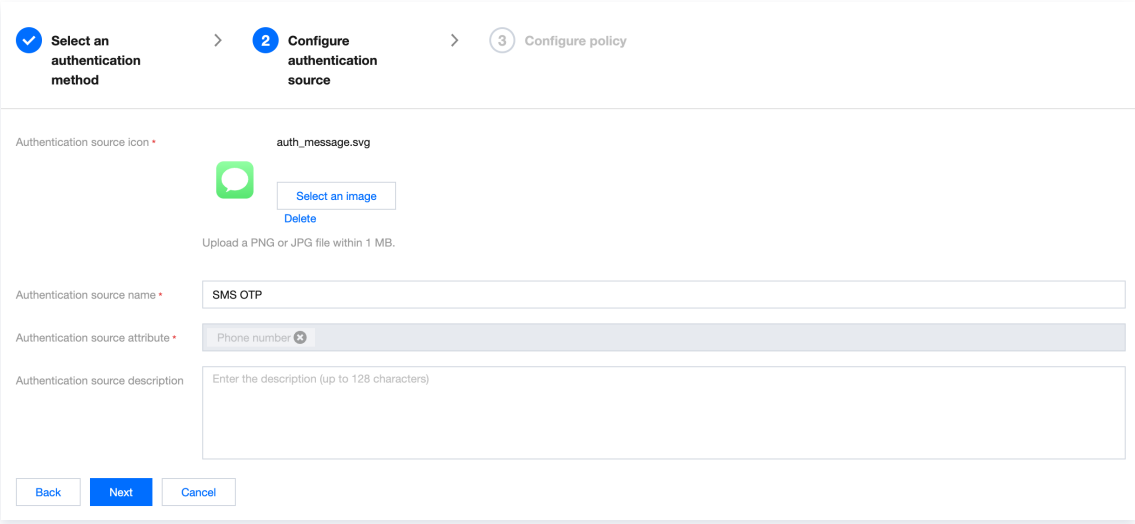
Scenario

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

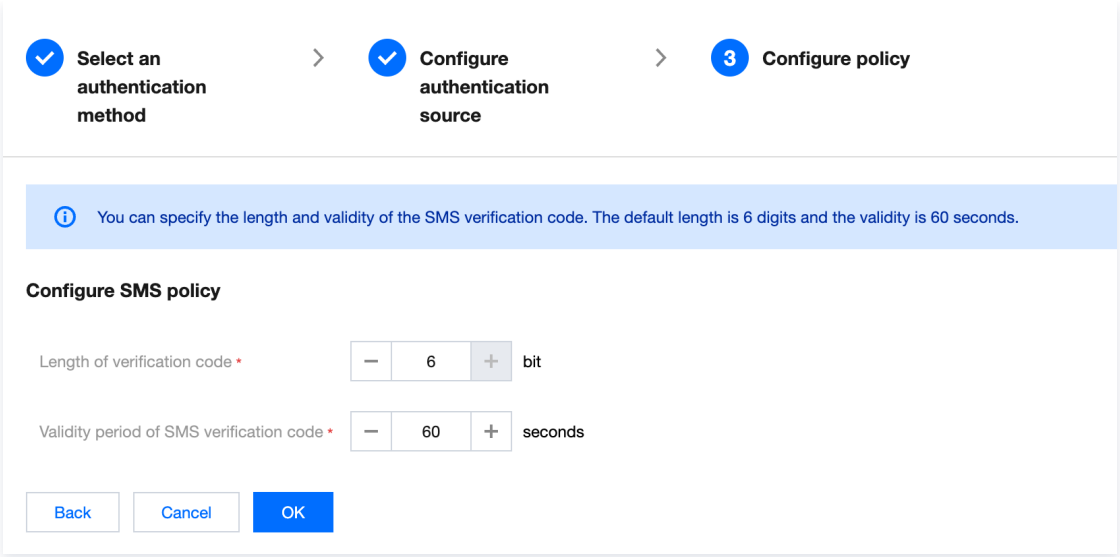
1. Log in to the Account Risk Control Platform console, and select **Authentication Management** > **General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, click **Create Authentication Source** to navigate to the Create Authentication Source page.
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.



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.



Email OTP

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

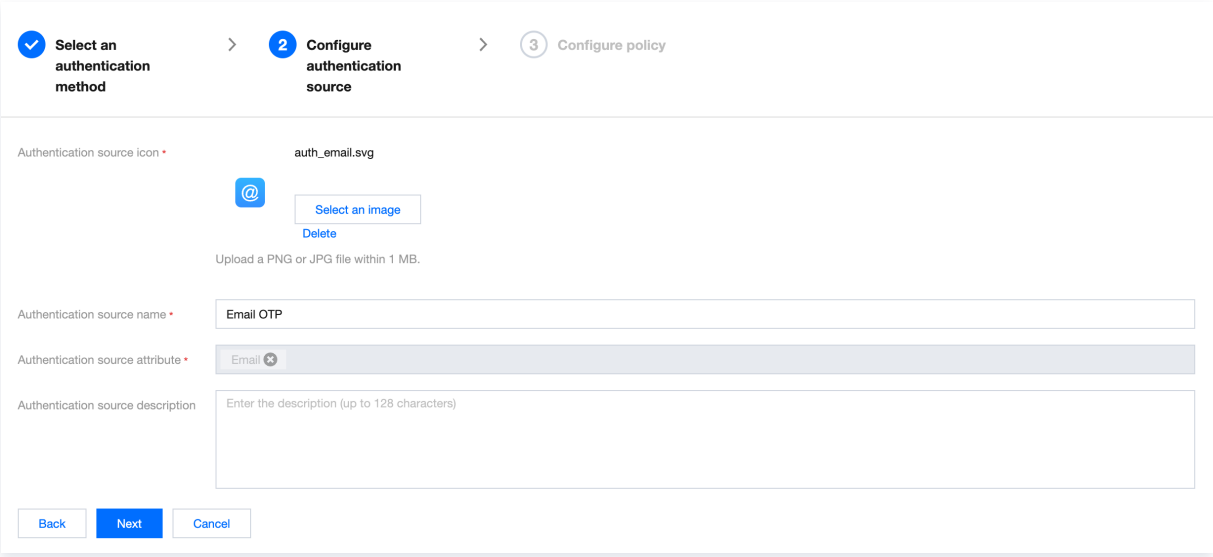
Scenario

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

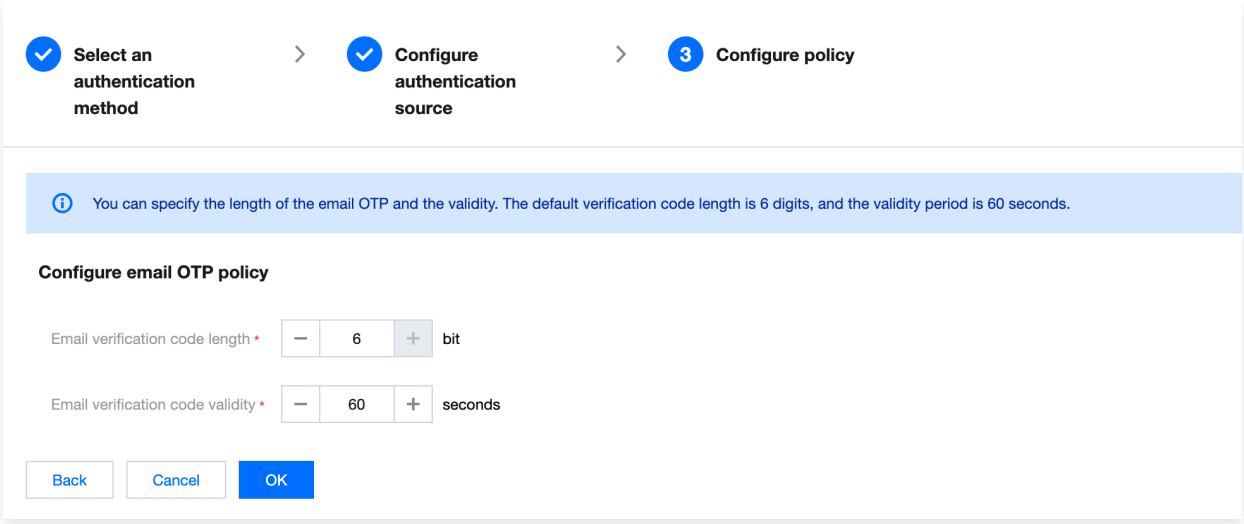
1. Log in to the Account Risk Control Platform console, select **Authentication Management** > **General Authentication Source** from the left navigation bar to access the General Authentication Source page.
2. On the General Authentication Source page, click **Create Authentication Source** to navigate 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.



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.



Editing an authentication source
Account and Password Authentication

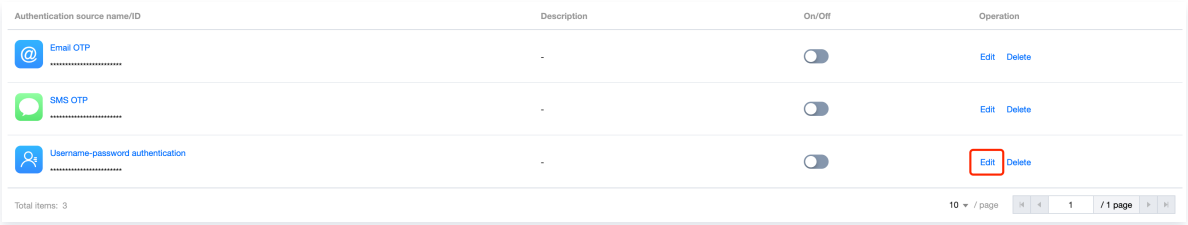
Last updated: 2023-09-04 11:37:33

Preparations

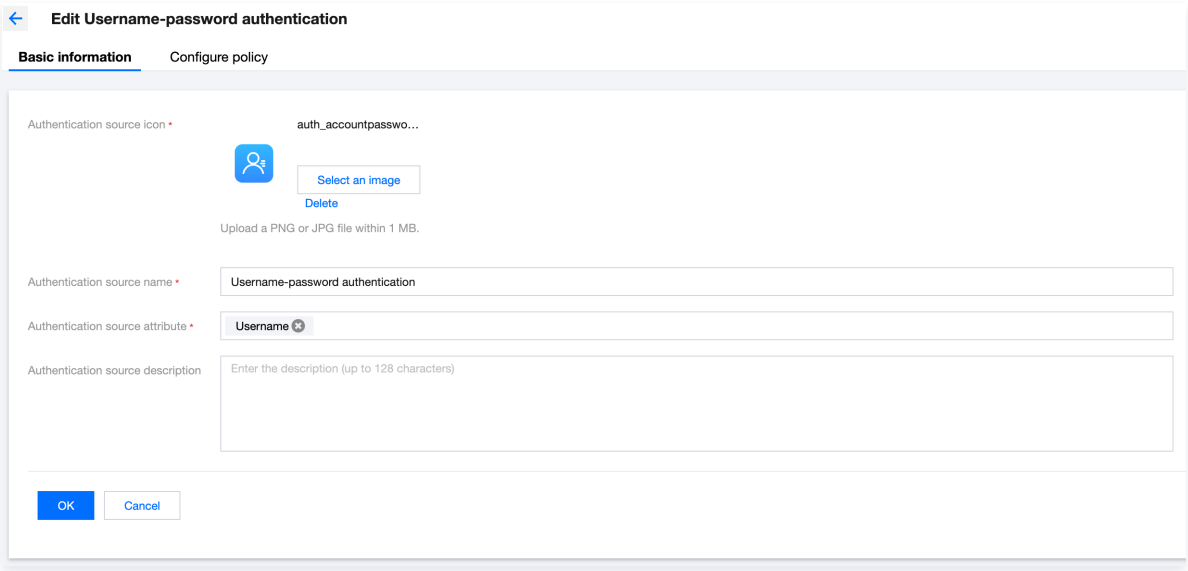
The enabled authentication source cannot be edited. It must be disabled before any modifications can be made.

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.



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



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

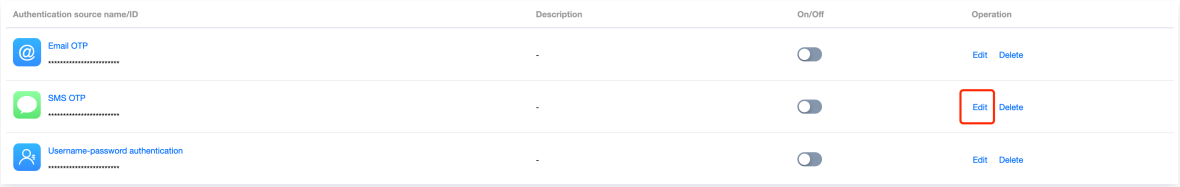
Last updated: 2023-09-04 10:34:52

Preparations

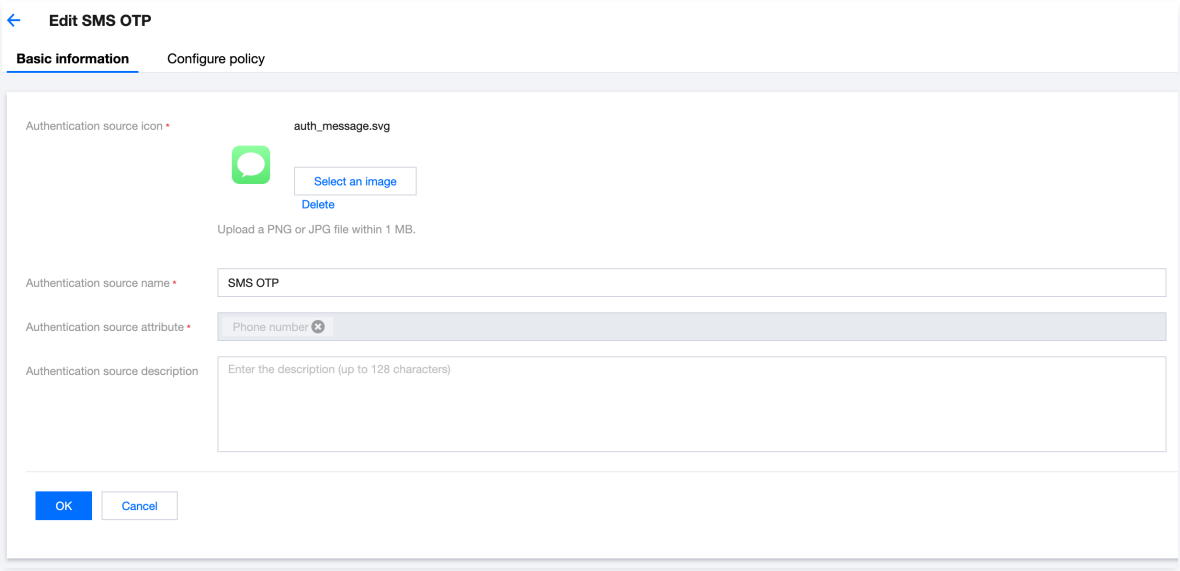
The enabled authentication source cannot be edited. It must be disabled before any modifications can be made.

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.

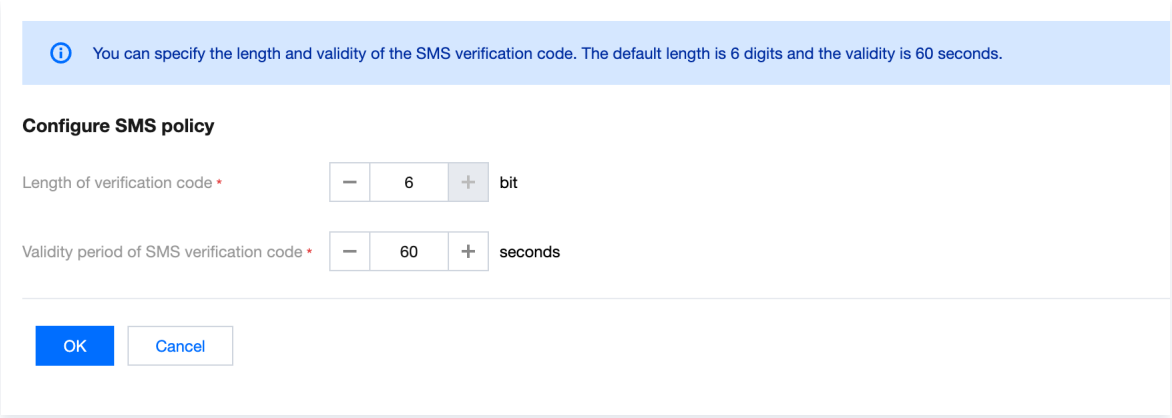


3. On the Basic Information page, modify the basic information as needed and click **Confirm** to update the basic information.



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.



Email OTP

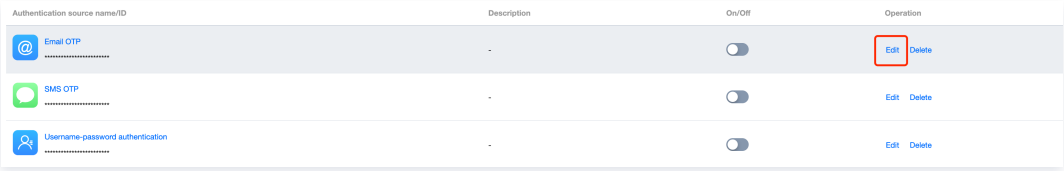
Last updated: 2023-09-04 11:42:26

Preparations

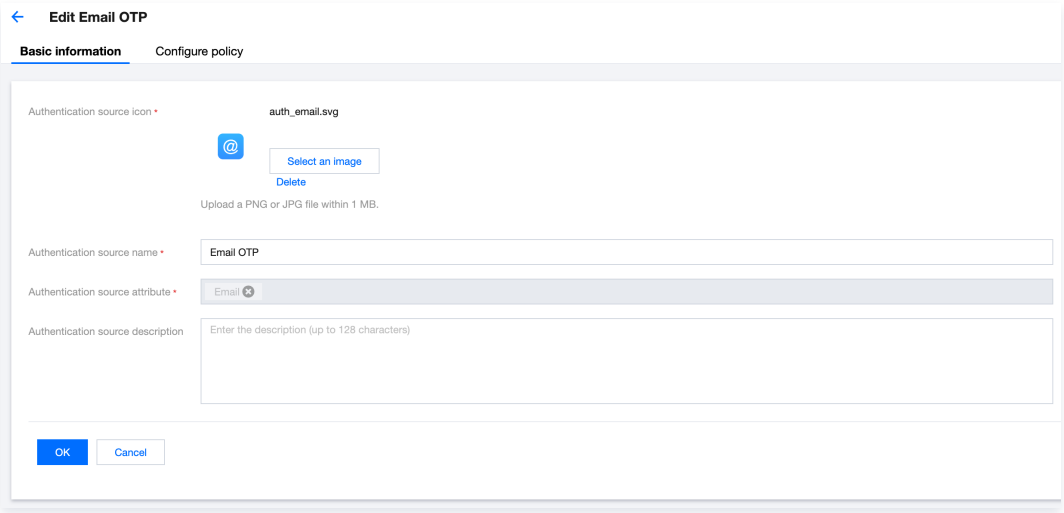
The enabled authentication source cannot be edited. It must be disabled before any modifications can be made.

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.

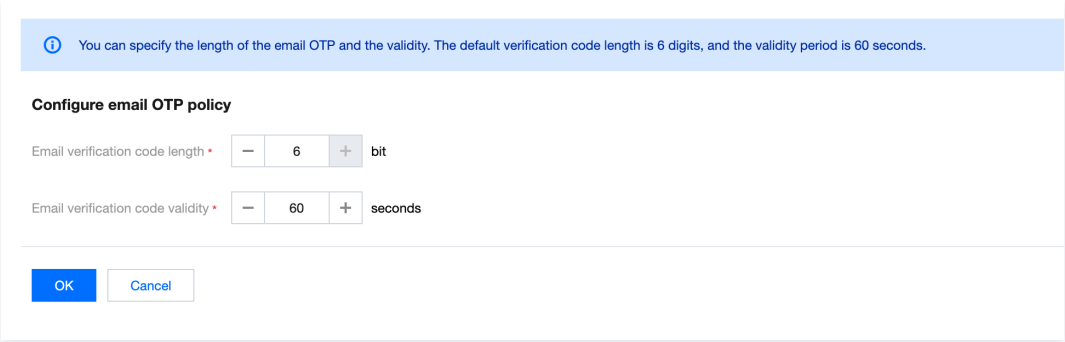


3. On the Basic Information page, modify the basic information as needed and click **Confirm** to update the basic information.



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.



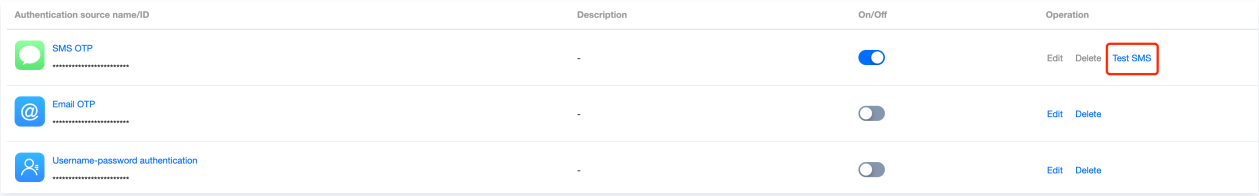
Testing an authentication source

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

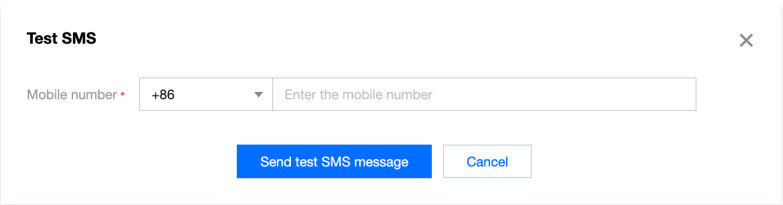
Test SMS

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.



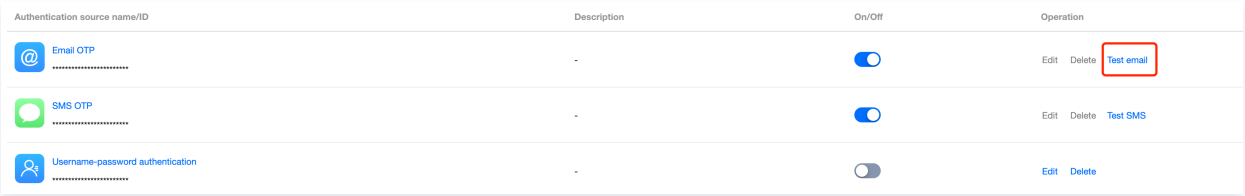
3. In the Test SMS pop-up window, enter the mobile number and click **Send Test SMS**. A test SMS will be sent to the user based on the configuration of the SMS OTP Authentication source.



Test 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.



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

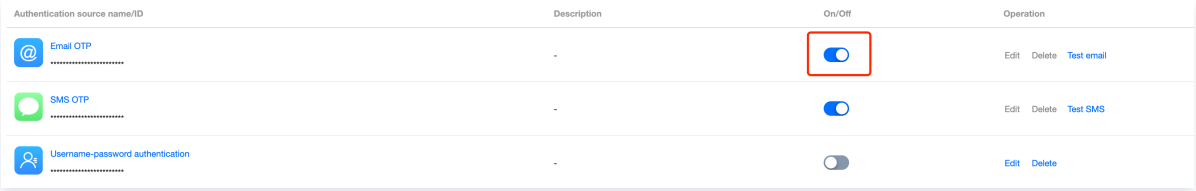
This document outlines the process of disabling and deleting an authentication source in the Account Risk Control console.

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

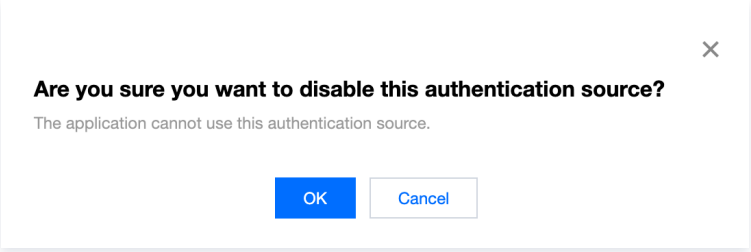
1. Log in to the Account Risk Control Platform console, and select **Authentication Management** > **General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, select the required authentication source and click  to trigger the "Confirm Closure" pop-up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



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.

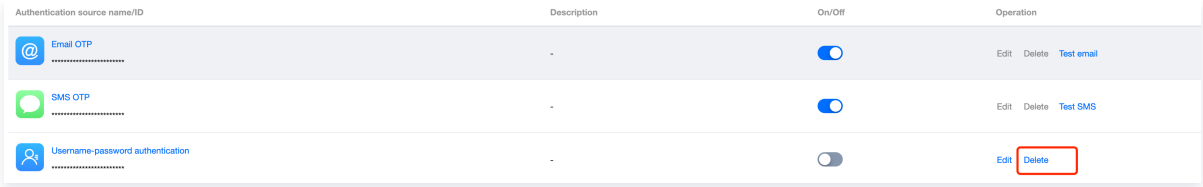


Deleting Authentication Source

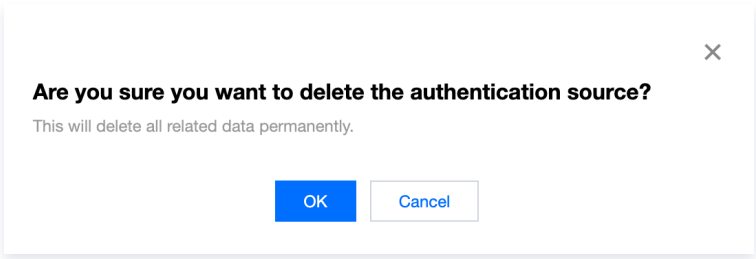
1. Log in to the Account Risk Control Platform console, and select **Authentication Management** > **General Authentication Source** from the left navigation bar.
2. On the General Authentication Source page, select the desired authentication source, click Delete, and a "Confirm Deletion" pop-up window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



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

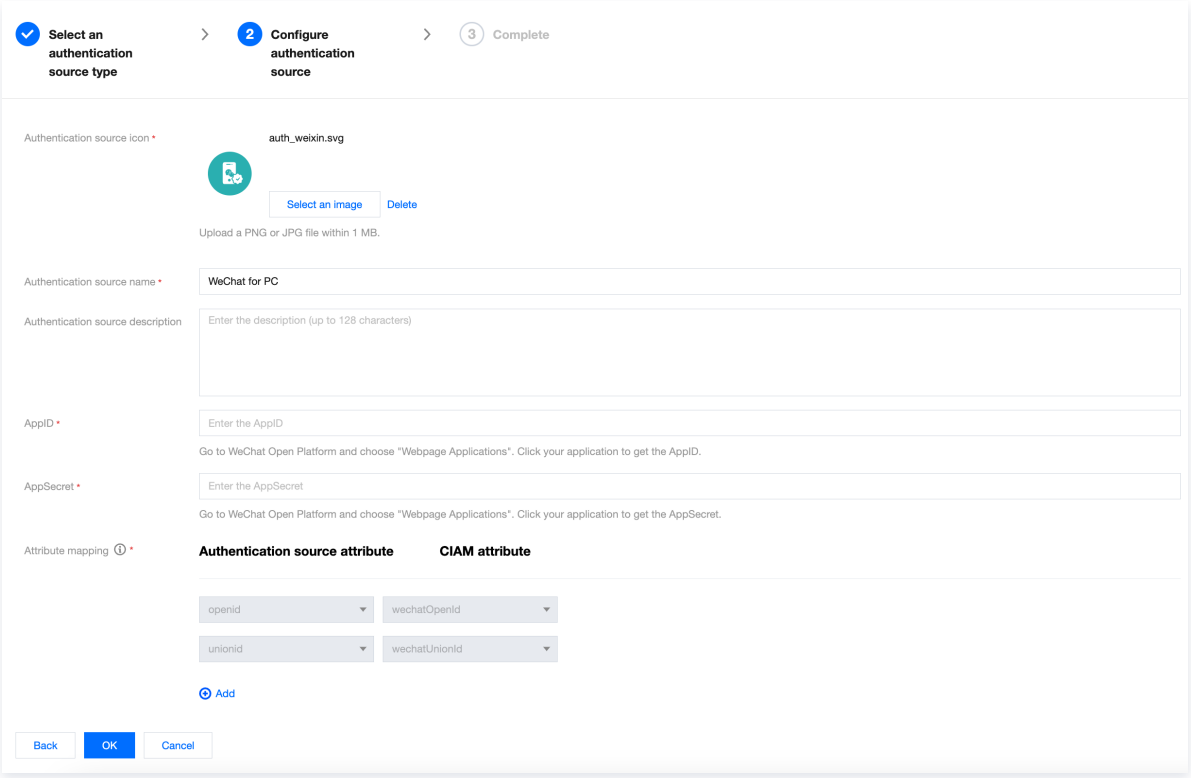
Last updated: 2023-09-04 10:36:57

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.



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

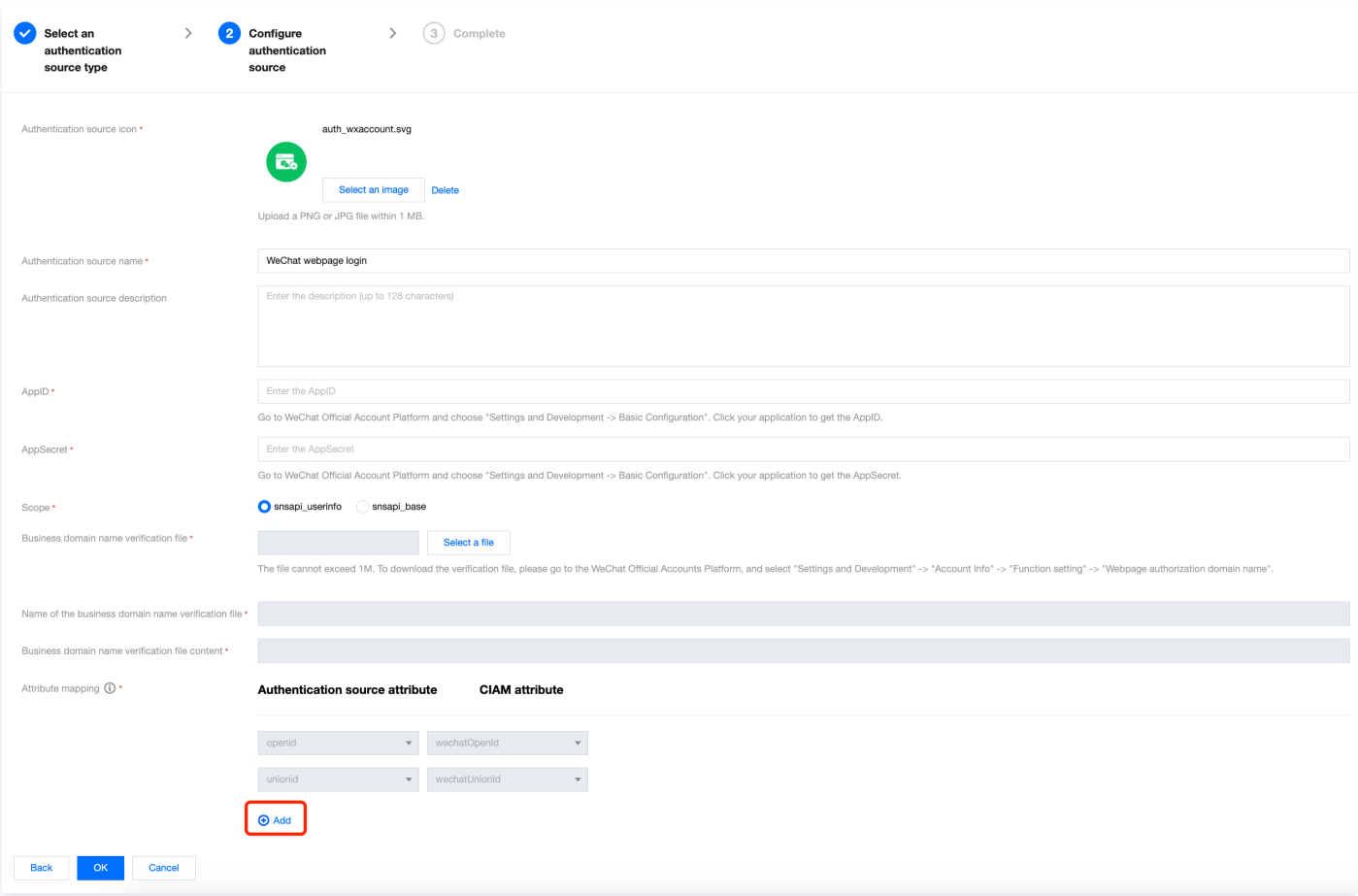
Last updated: 2023-09-04 10:37:04

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.



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

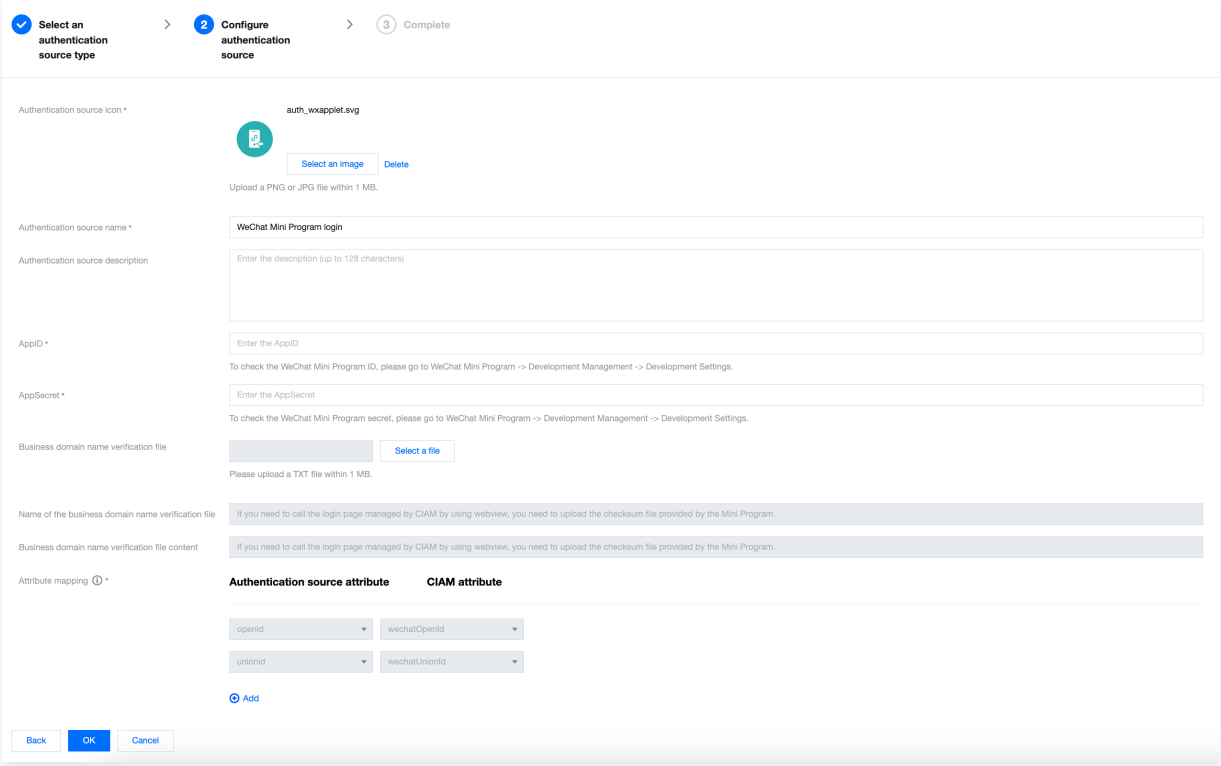
Last updated: 2023-09-04 10:37:10

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.



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

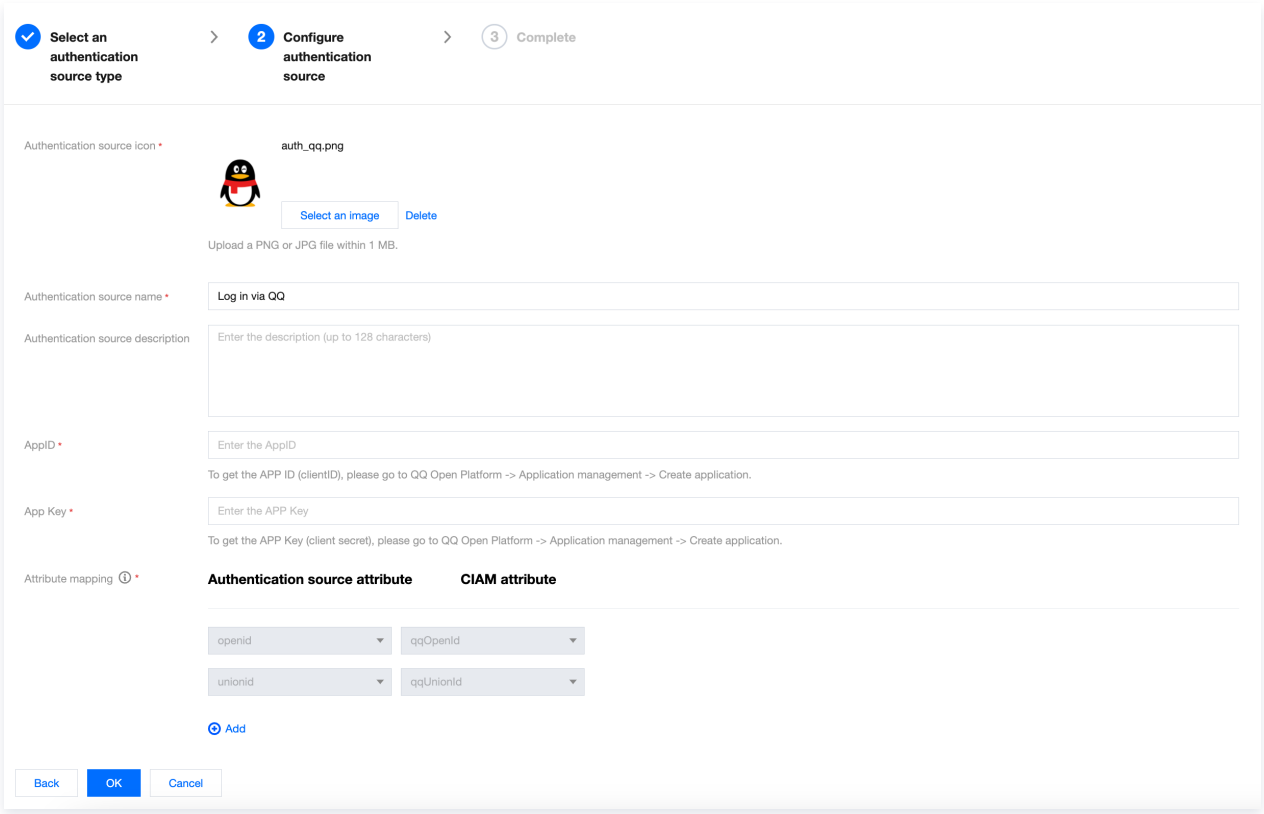
Last updated: 2023-09-04 10:37:16

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.



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

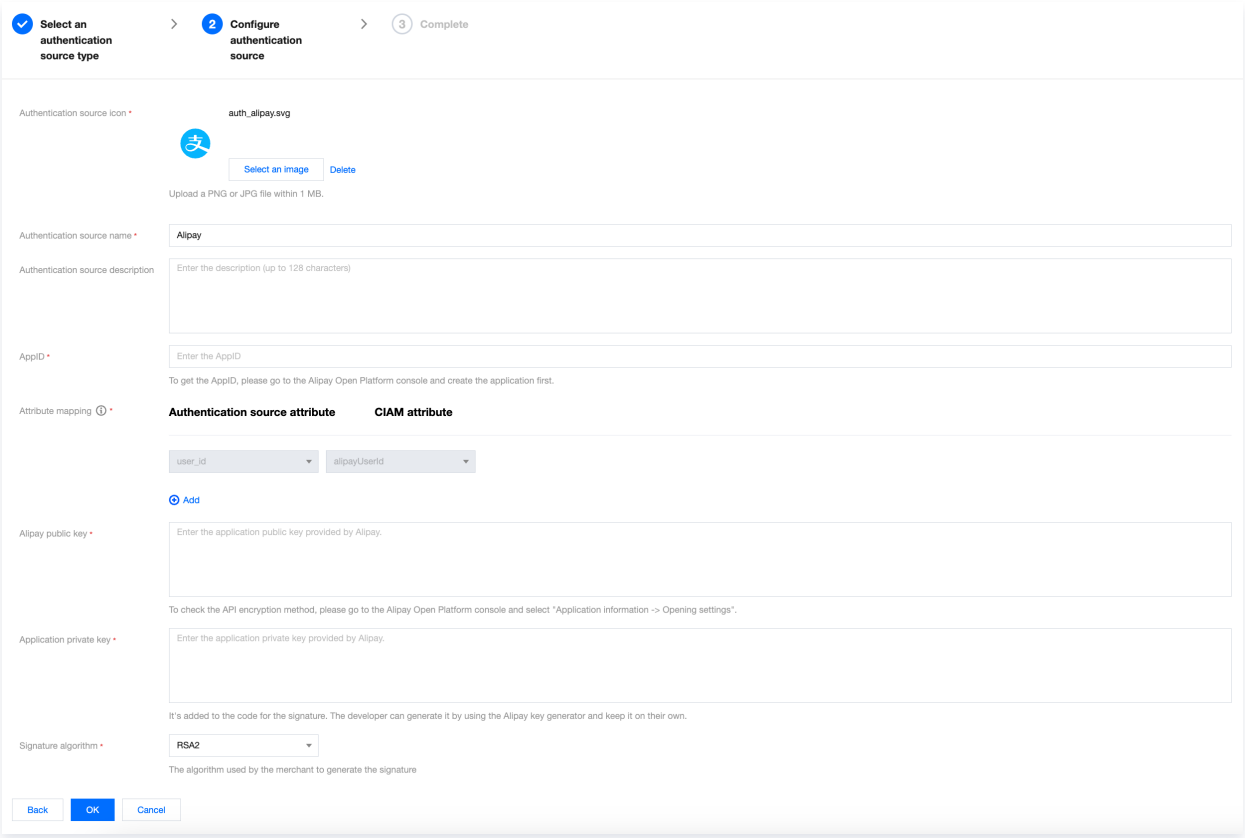
Last updated: 2023-09-04 10:37:27

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.



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

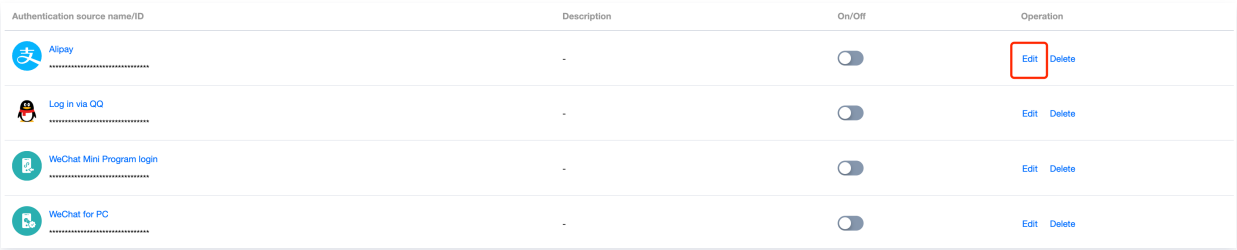
Last updated: 2023-09-04 10:38:48

Preparations

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

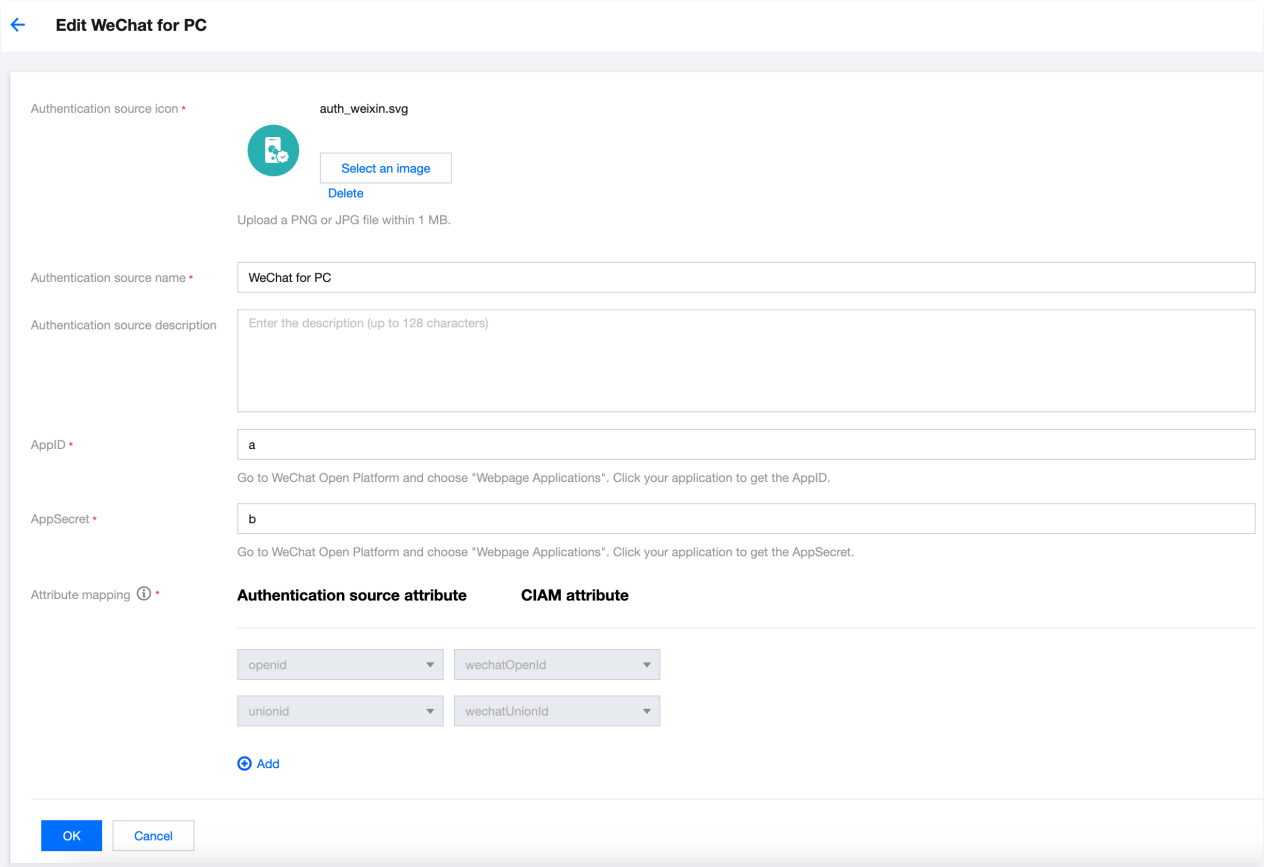
Instructions

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.



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.



Disabling or deleting an authentication source

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

Scenario

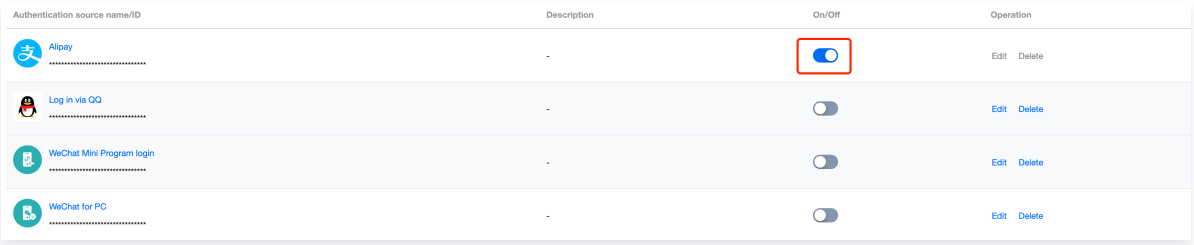
This document outlines the process of disabling and deleting an authentication source in the Account Risk Control console.

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

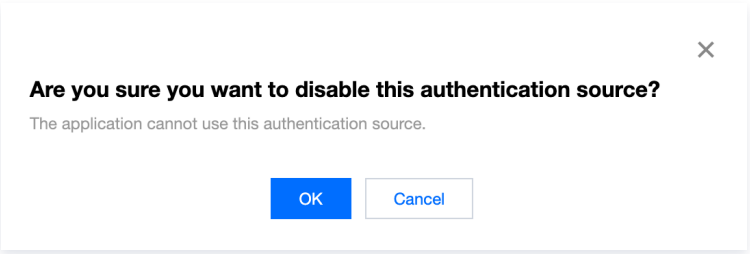
1. Log in to the Account Risk Control Console, and select **Authentication Management** > **Social Authentication Source** from the left navigation bar.
2. On the Social Authentication Source page, select the desired authentication source and click to trigger the "Confirm Closure" pop-up window.



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.

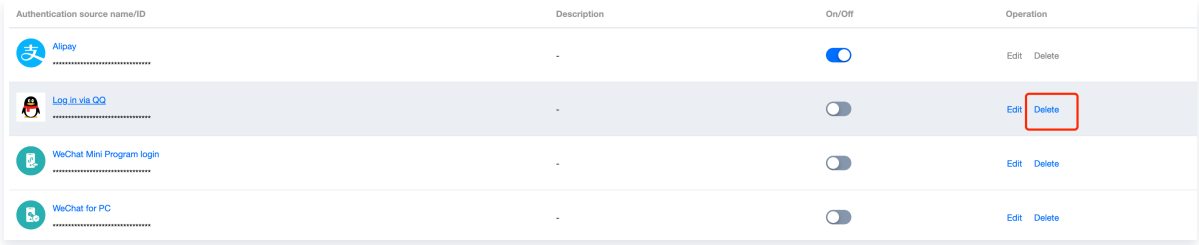


Deleting Authentication Source

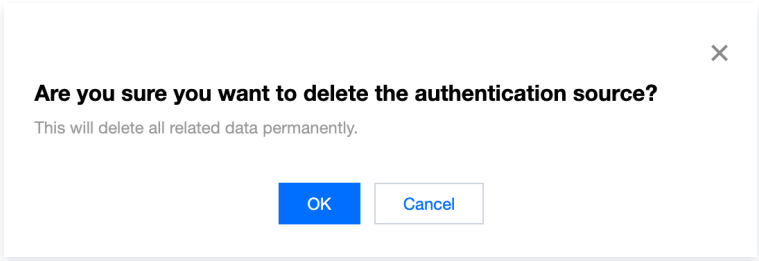
1. On the Social Authentication Source page, select the desired authentication source and click **Delete**. A confirmation pop-up window will appear.

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.



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

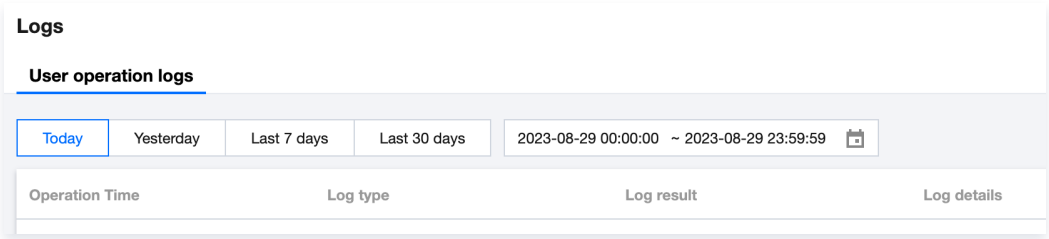
Scenario

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.

Custom Settings
Template Configuration
SMS templates

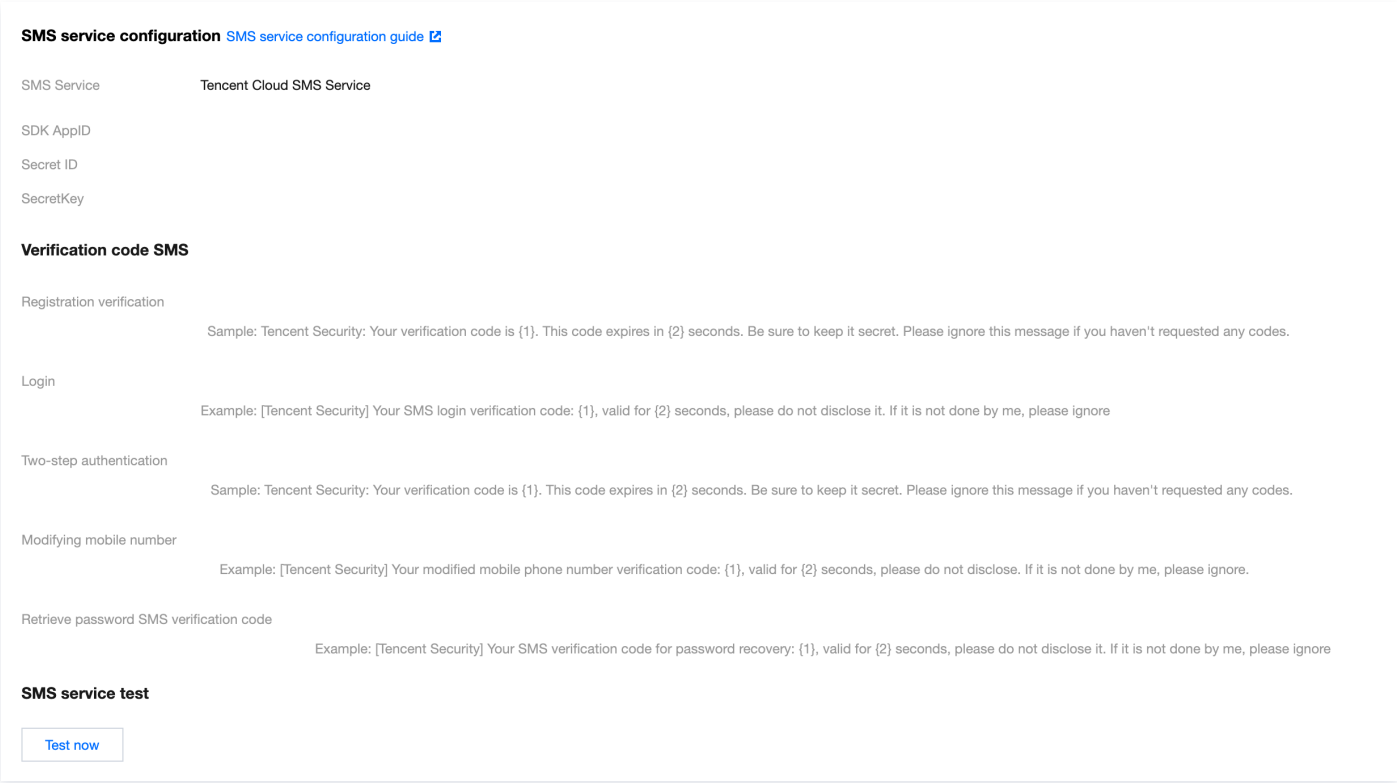
Last updated: 2023-09-04 10:39:20

Scenario

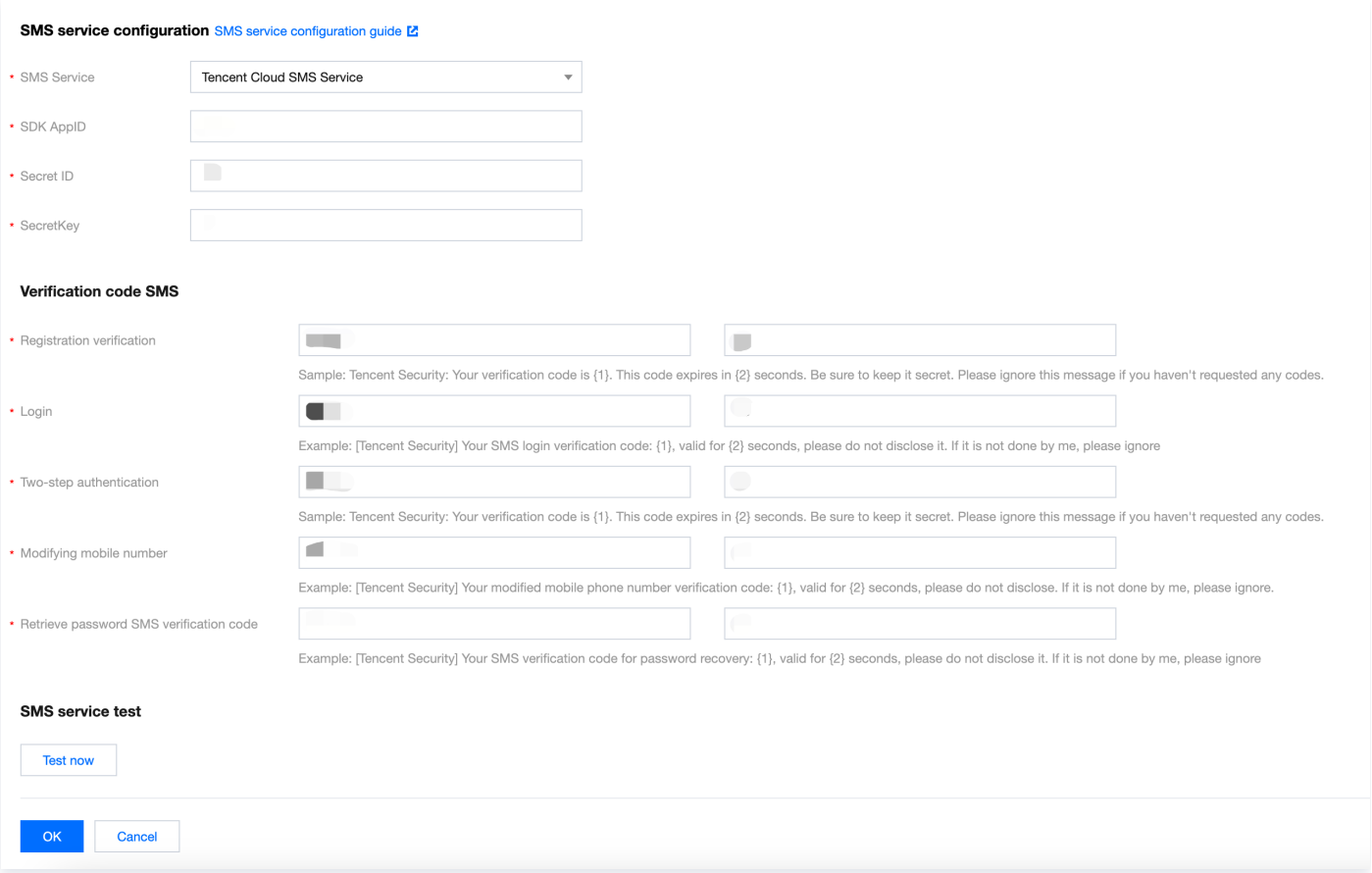
By default, the Account Risk Control Platform provides each tenant with 50 free SMS messages. Once this quota is exceeded, the platform will suspend SMS delivery for the tenant, affecting console test messages, portal SMS OTP authentication, and MFA two-factor authentication. To ensure the normal operation 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.



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**.

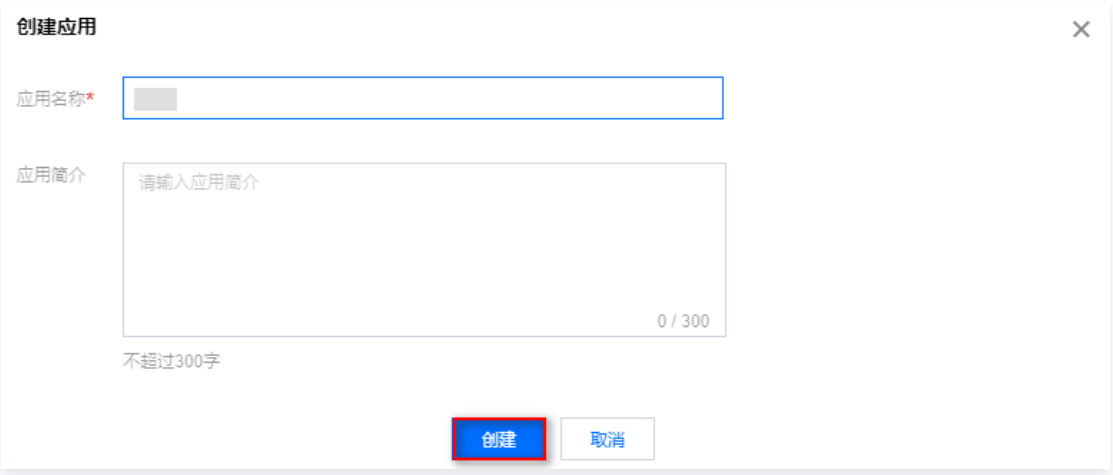


Note:
Different SMS services require different configuration parameters. Currently, the platform only supports **Tencent Cloud SMS Service**, but will gradually support the configuration of other SMS services. The following are the relevant parameters needed to configure Tencent Cloud SMS Service.

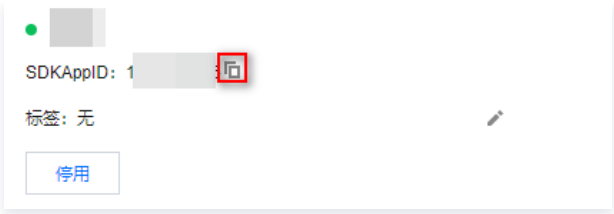
SMS service configuration

Obtaining the SDK AppID

1. Log in to the Tencent Cloud SMS Console, and in the left navigation bar, select **Application Management** > **Application List**.
2. On the Application List page, click **Create Application**, enter the application name and description, and click **Create** to complete the application creation process.

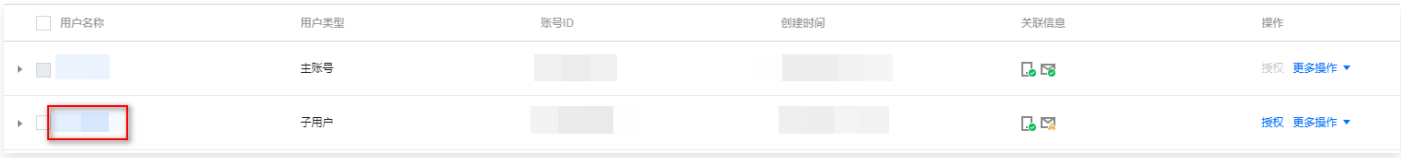


3. On the application list page, select the desired application and click to obtain the SDK AppID for that application.



Obtaining the SecretId and SecretKey

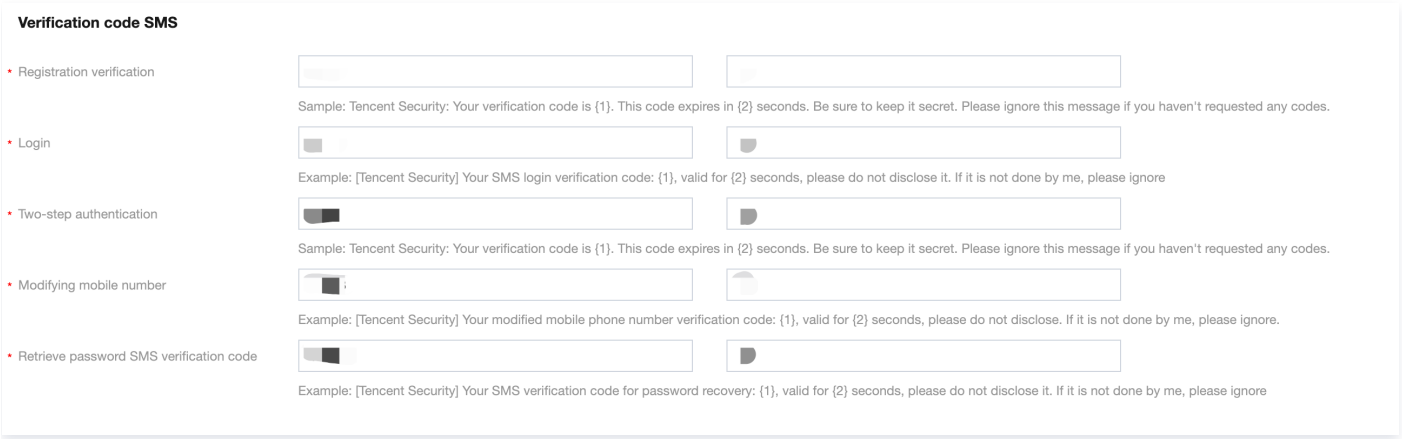
1. Log in to the Access Management Console, and in the left navigation bar, select **Users** > **User List**.
2. On the User List page, select the desired sub-account and click on the **Username** to enter the User Details page.



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

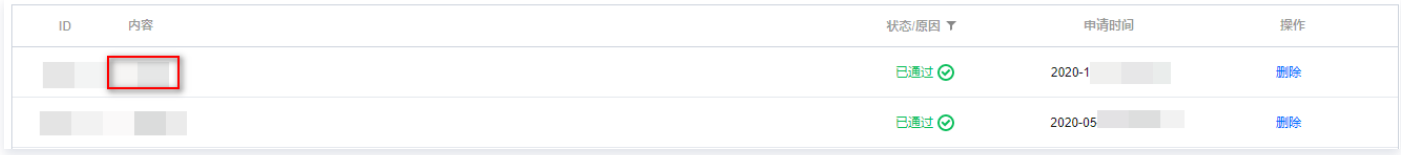
Setting up an SMS template requires obtaining the SMS signature and SMS template ID needed for SMS login. The acquisition method is as follows:



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**.

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



Retrieving SMS Template ID

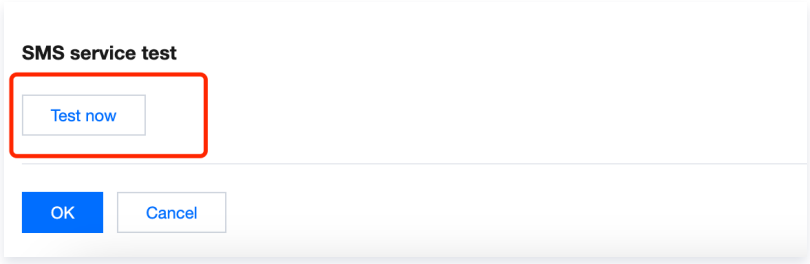
1. Log in to the SMS Service Console, and in the left navigation bar, select **Domestic SMS** > **Body Template Management**.
2. On the Body Template Management page, click **Create Body Template**, fill in the relevant parameters, and click **OK** to confirm.

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

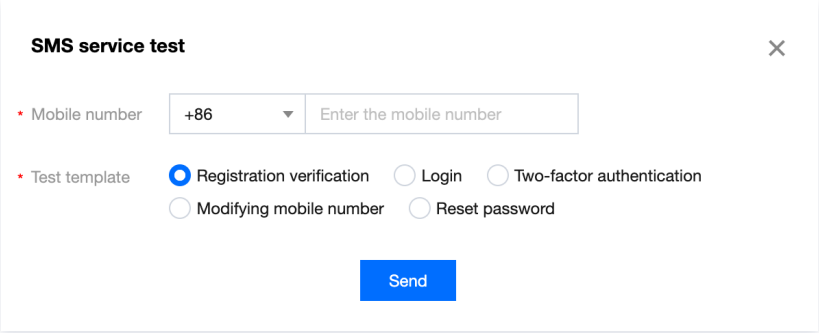
Testing SMS Service

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

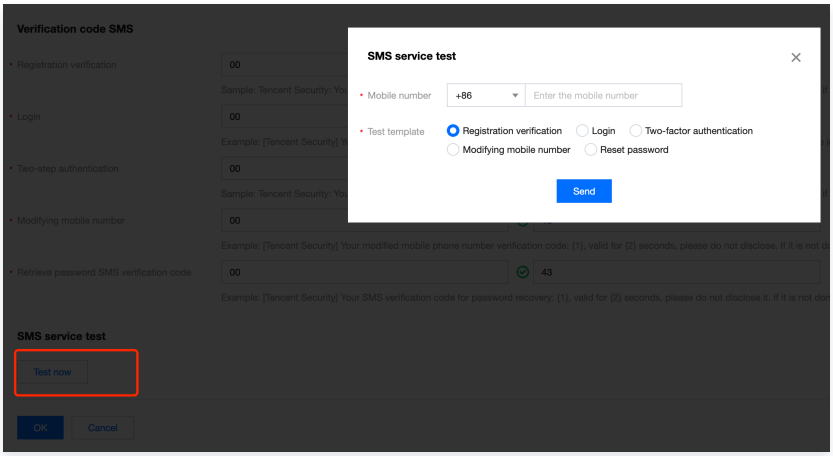
1. On the SMS Template Configuration Edit page, click on **Test SMS Service Now** to open the test window.



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.



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.



Email templates

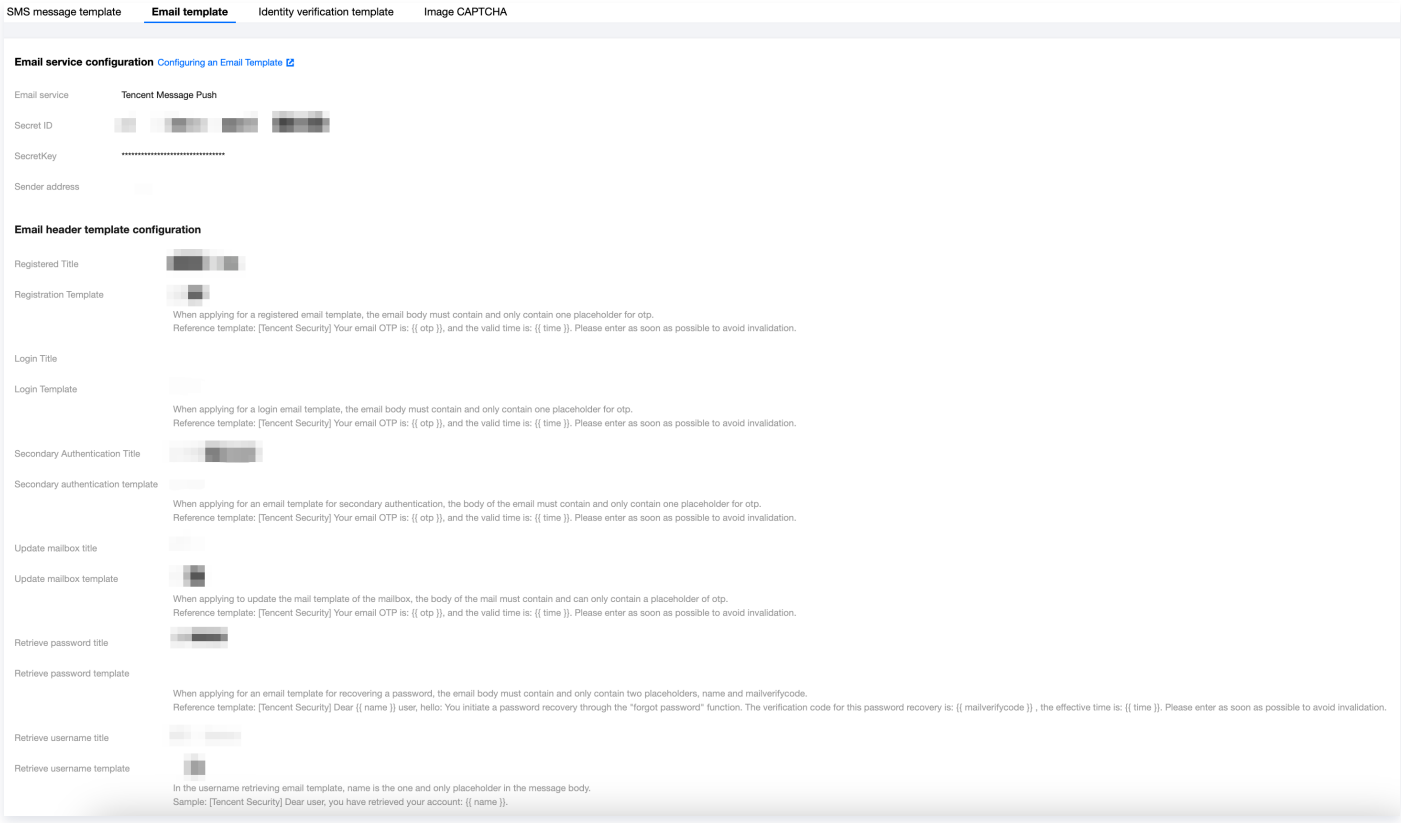
Last updated: 2023-09-04 10:39:27

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.



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**.

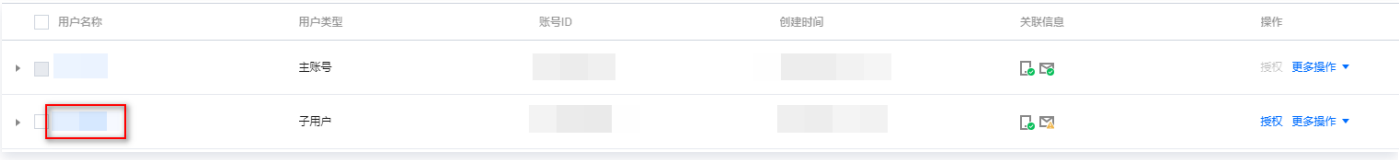
> **Note**
> Different email services require different configuration parameters. Currently, the platform **only supports Tencent Email Push**, but will gradually support the configuration of other email services. The following are the relevant parameters needed to configure the Tencent Cloud Email Service.

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.



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.

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.

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.

Email template settings

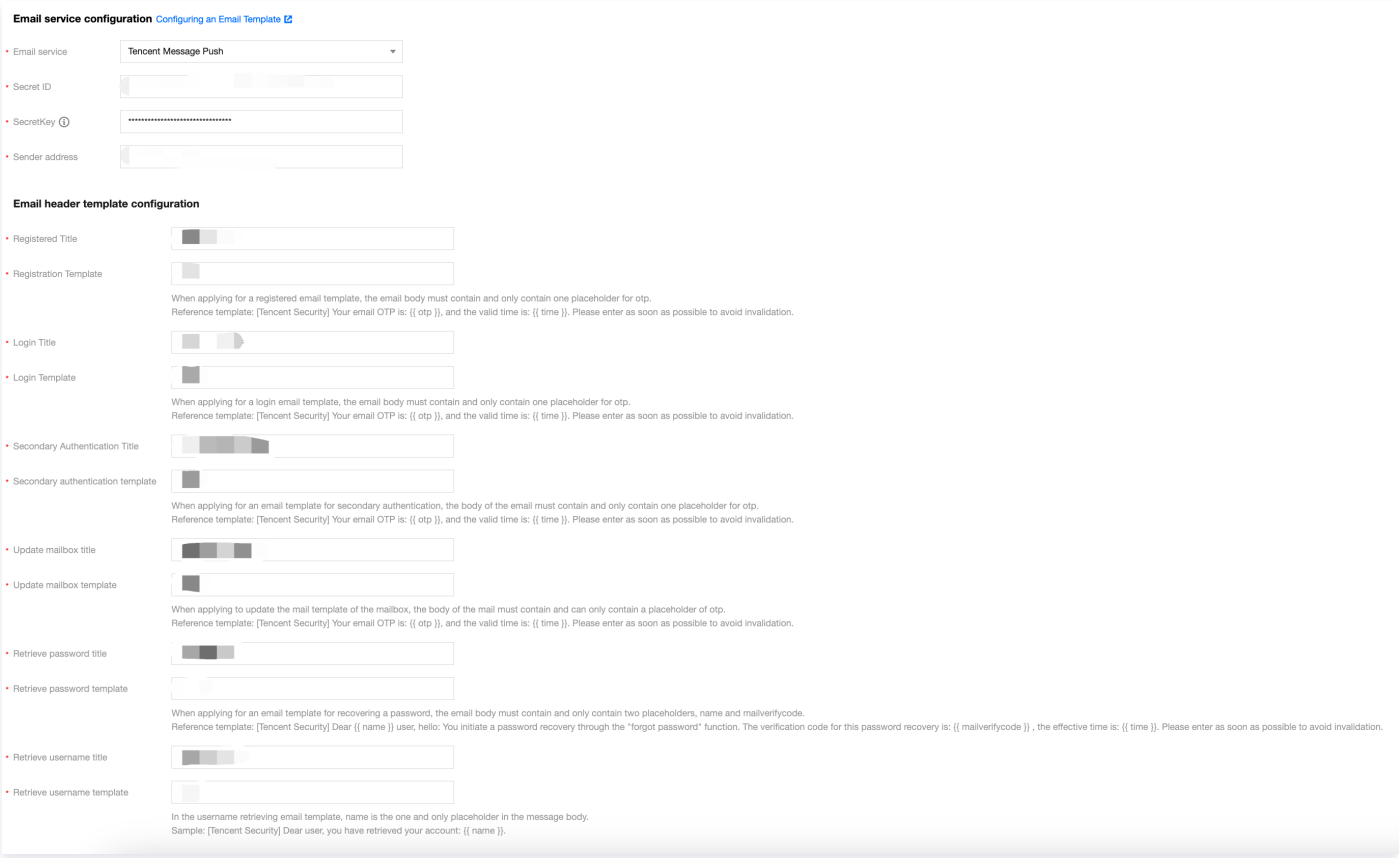
1. On the Send Mail Template page, click **New**, configure the relevant parameters, and click **Submit**. This template can then be used to invoke the email push service.

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 }}.

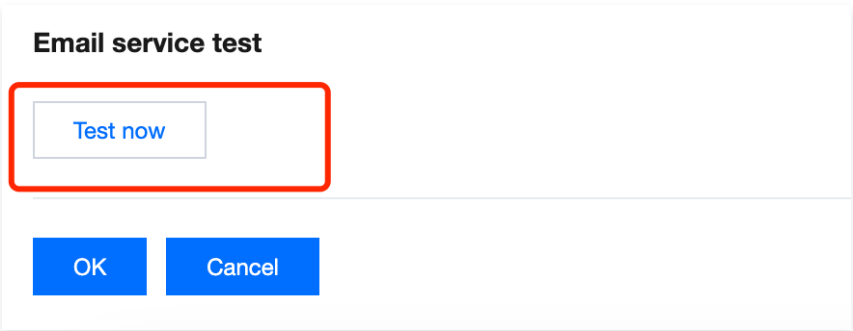
2. On the Sending Template page, you can see the template that was just created. Copy the Sending Template ID.

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.



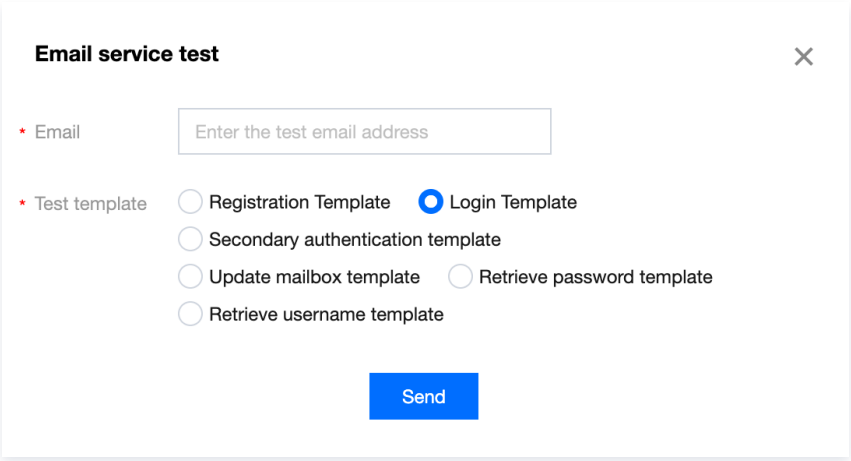
Testing Email Service

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.



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.



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

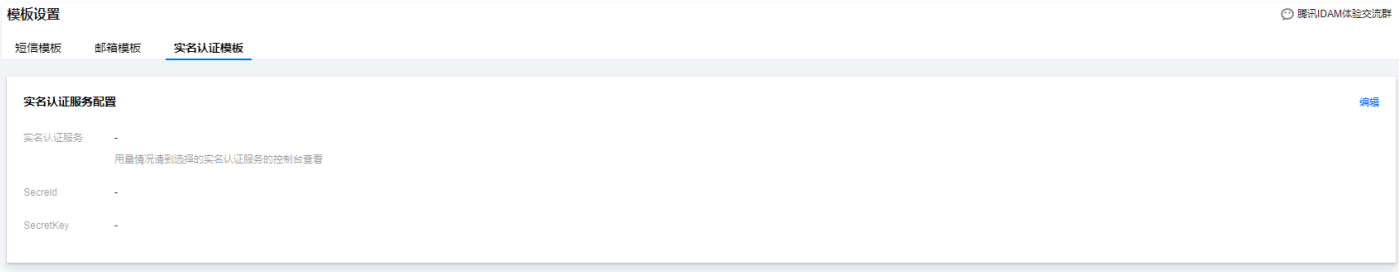
Last updated: 2023-09-04 10:39:32

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.



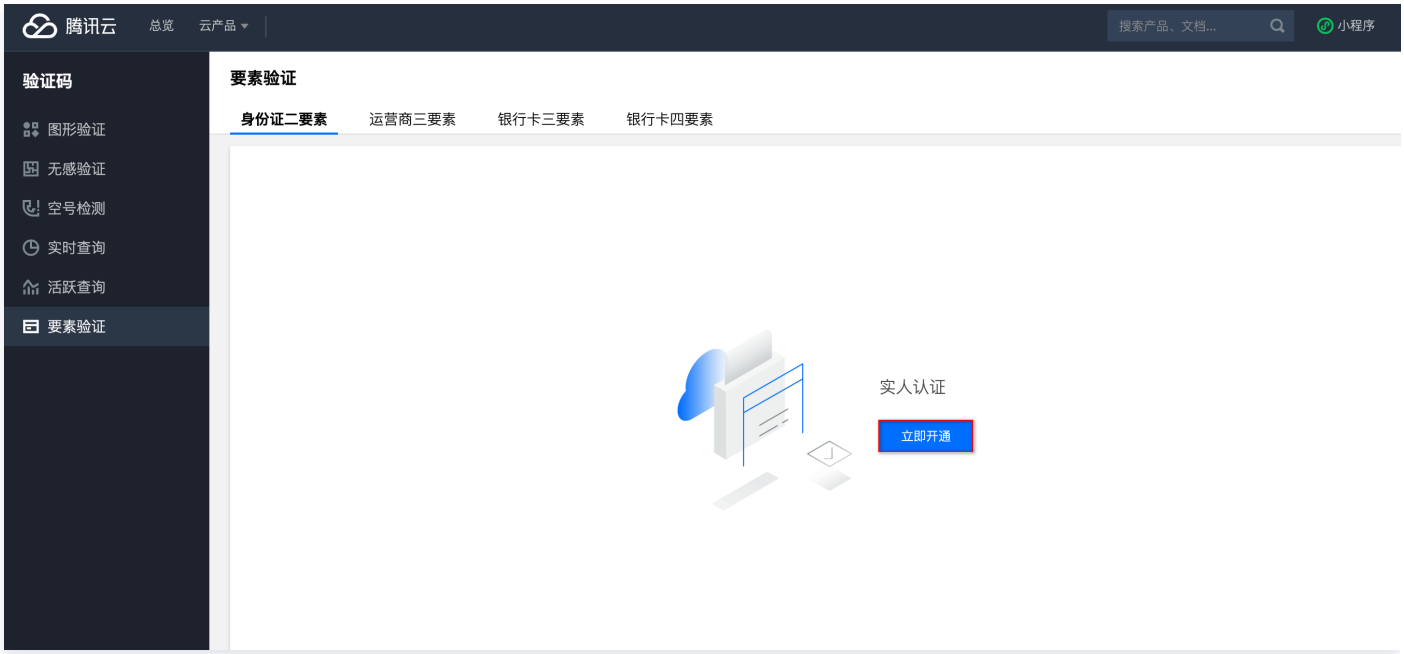
3. On the Identity Verification Template page, click **Edit** in the top-right corner of the interface.
4. On the editing page, select the identity verification service, enter the SecretId and SecretKey, and click **Confirm**.

> **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.

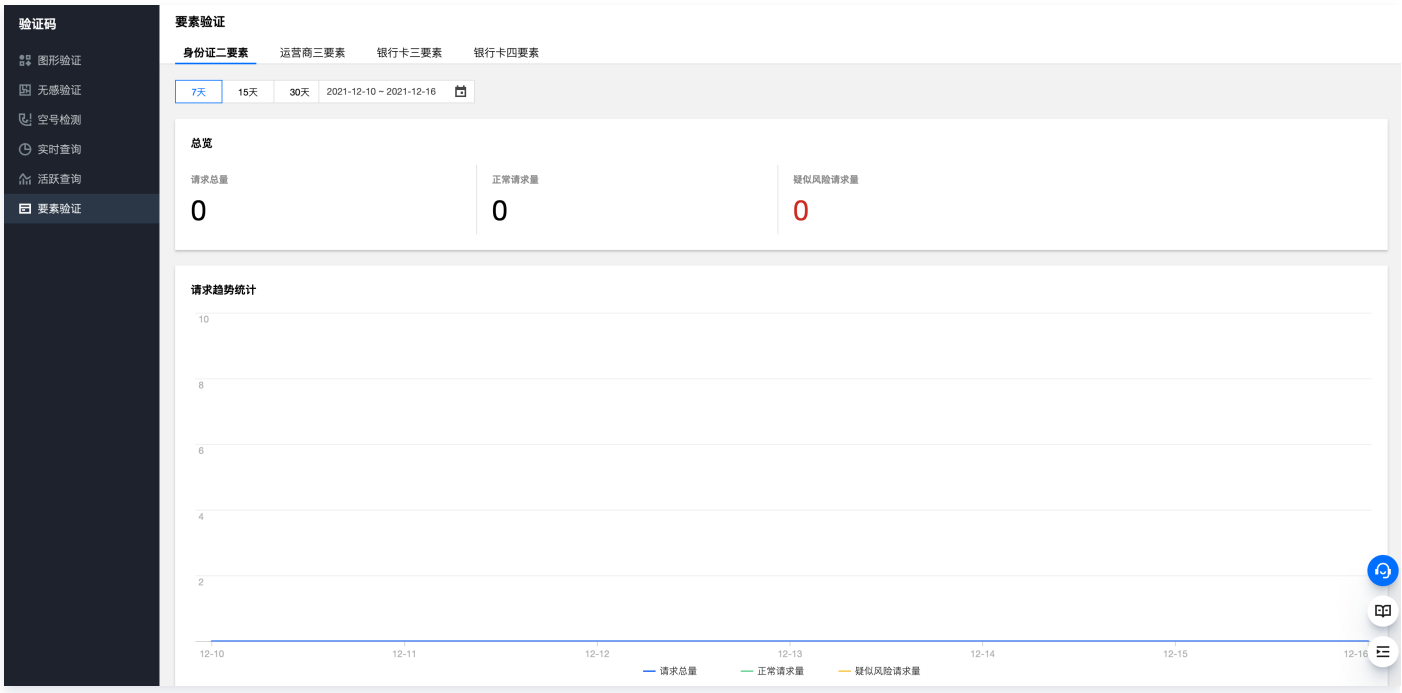
Activating the Skyeye Identity Verification Service

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.



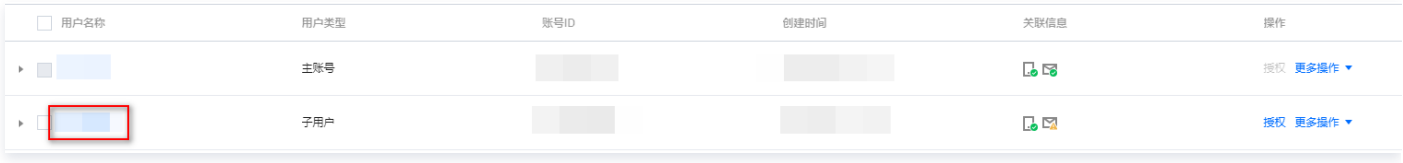
3. After successful activation, you can view usage data in the console after invoking the identity verification service.



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.



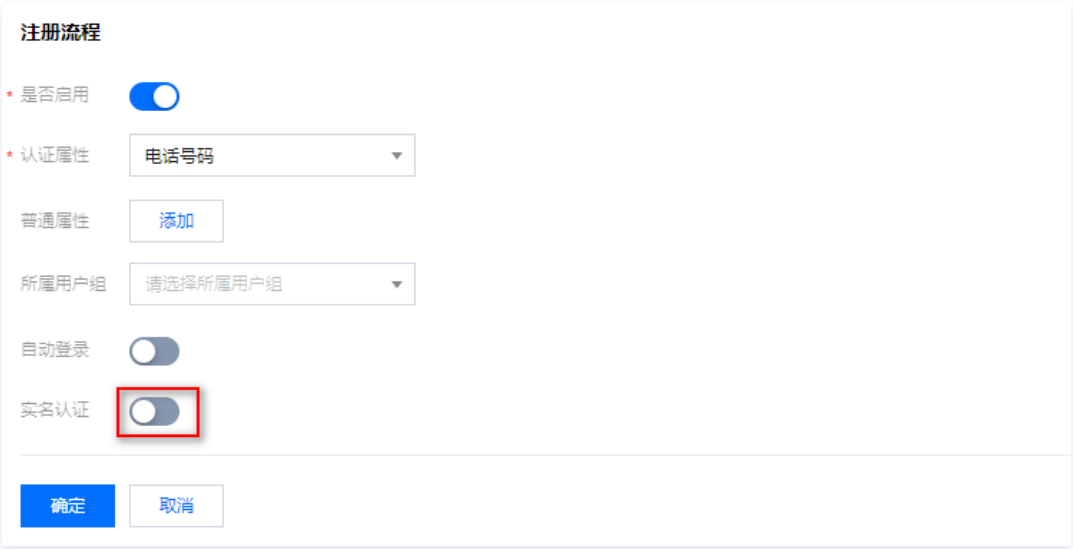
3. On the User Details page, click **API Key**, select the required key, and click to obtain the SecretId for this sub-account. Click **Show**, and after successful identity verification, you can obtain the SecretKey for this sub-account.

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**.

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

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



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

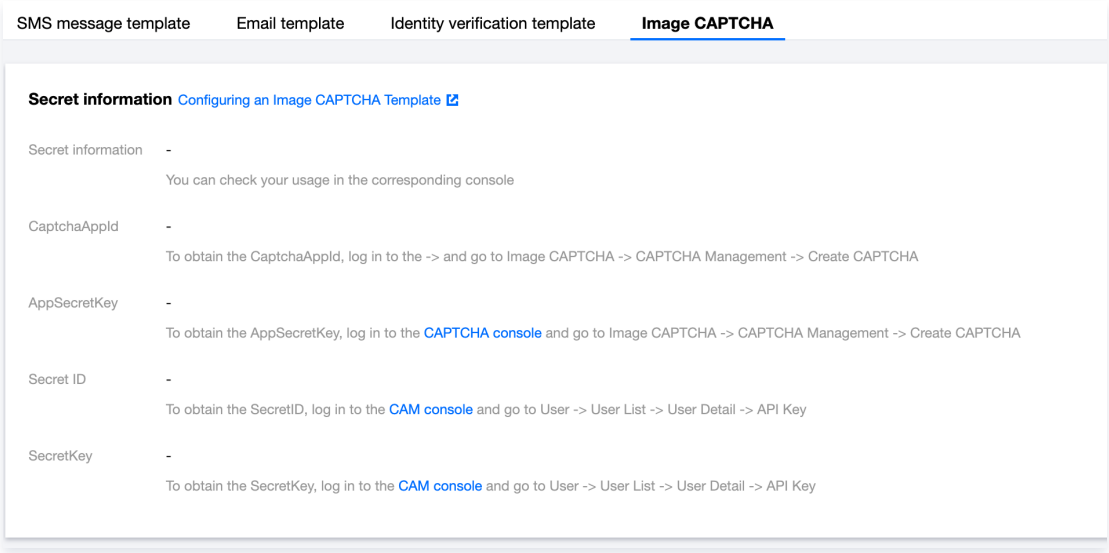
Last updated: 2023-09-04 10:39:38

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.

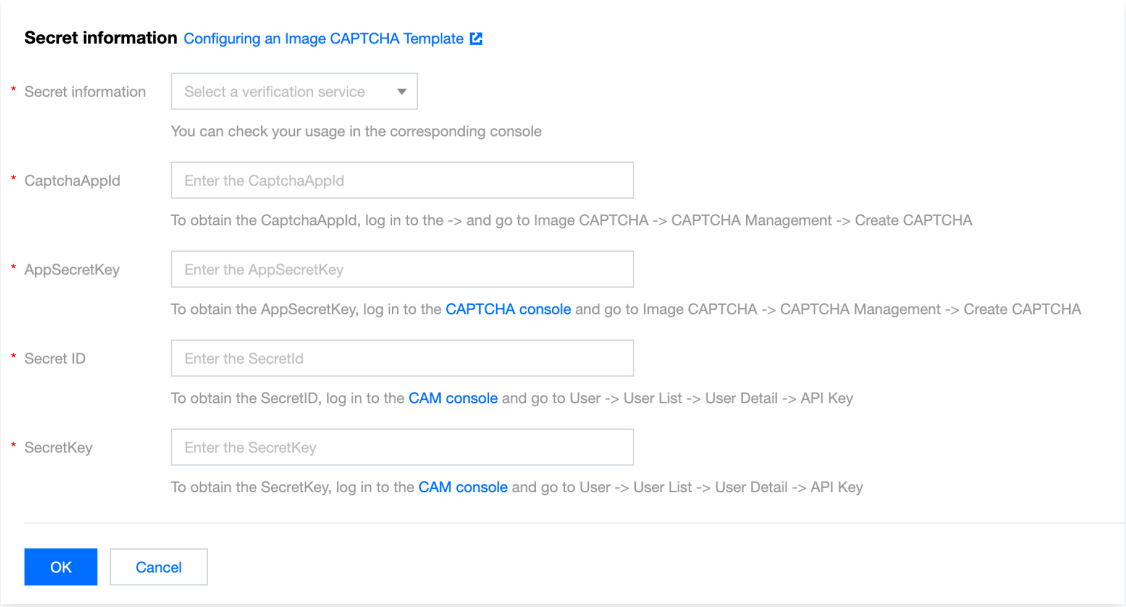


Image Verification Service Configuration

Obtain CaptchaAppId and AppSecretKey

> **Note**
> To obtain the CaptchaAppId and AppSecretKey, you must first purchase the CAPTCHA Package.

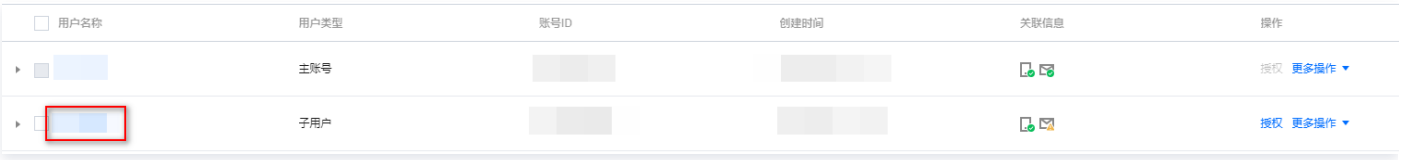
1. Log in to the CAPTCHA console, and select **Image Verification** > **Verification Management** from the left sidebar.
2. On the Verification Management page, click **Create Verification**.

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.



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.