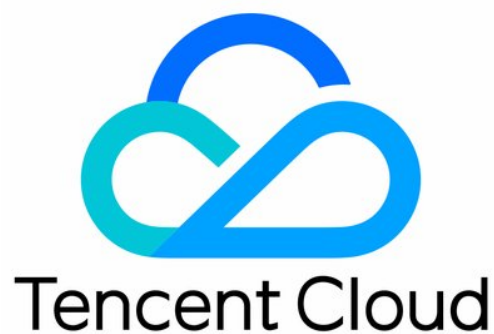


# **Customer Identity and Access Management Operation Guide Product Documentation**



## Copyright Notice

©2013-2023 Tencent Cloud. All rights reserved.

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

## Trademark Notice



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

## Service Statement

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

# Contents

## Operation Guide

### User pool management

- Creating a user pool

- Switching user pools

- Setting the default user pool

- Editing a user pool

- Deleting a user pool

### User management

#### Custom attributes

- Creating a custom attribute

- Editing a custom attribute

- Viewing custom attributes

- Deleting a custom attribute

- Creating a user

- Viewing user details

- Editing user attributes

- Deleting a user

- Resetting a password

- Freezing or locking users

- User group management

### Application management

- Creating an application

- Configuring an application

### Authentication management

#### General authentication sources

- Creating an authentication source

- Username-password authentication

- SMS OTP

- Email OTP

- Editing an authentication source

- Username-password authentication

- SMS OTP

- Email OTP

- Testing an authentication source

- Disabling or deleting an authentication source

Audit management

Custom settings

Domain settings

Template settings

SMS templates

Email templates

# Operation Guide

## User pool management

### Creating a user pool

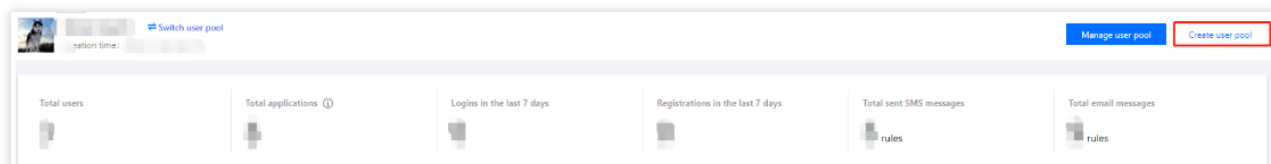
Last updated : 2023-12-22 11:42:07

## Scenarios

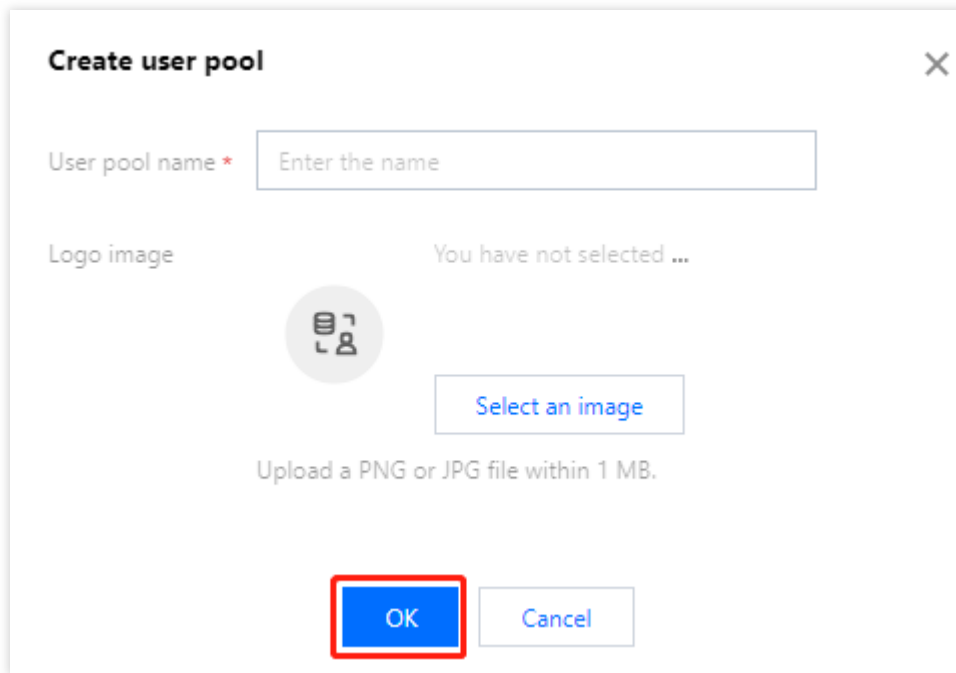
The user pool is the first-level directory of Customer Identity and Access Management (CIAM). All the data of users, custom attributes, applications, and authentication sources are isolated by the user pool. Before using CIAM for the first time, you need to create a user pool. The platform allows you to configure multiple user pools.

## Steps

1. Log in to the [CIAM console](#) and select **Overview** in the left navigation pane.
2. If you are logging in to CIAM for the first time and no user pool is created, you can click **Create Now** to experience the quick create feature. The feature automatically creates demo data, including the data of applications and authentication sources.
3. On the **Overview** page, click **Create user pool** in the upper right corner.



4. In the **Create user pool** window displayed, complete the information, and then click **OK**.



The screenshot shows a dialog box titled "Create user pool" with a close button (X) in the top right corner. It contains the following elements:

- A text input field labeled "User pool name \*" with a red asterisk and a placeholder text "Enter the name".
- A section for "Logo image" with the text "You have not selected ...".
- A circular icon representing a user pool logo.
- A button labeled "Select an image" in blue text.
- A note: "Upload a PNG or JPG file within 1 MB."
- At the bottom, two buttons: "OK" (highlighted with a red border) and "Cancel".

**Parameter description:**

User pool name: This field cannot be empty. The name must be unique and cannot exceed 128 characters.

Logo image: Upload a PNG or JPG file within 1 MB.

# Switching user pools

Last updated : 2023-12-22 11:42:07

## Scenarios

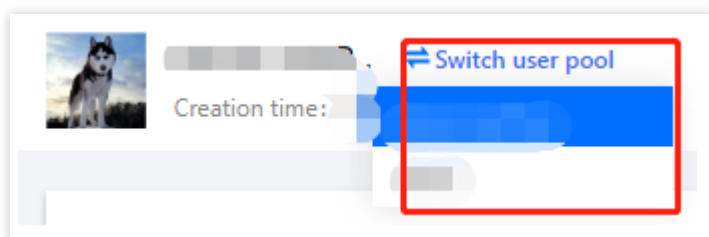
Customer Identity and Access Management (CIAM) supports multiple user pools. Administrators can switch to different user pools to manage and configure them.

## Steps

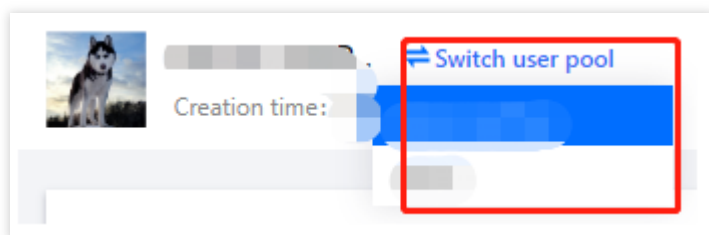
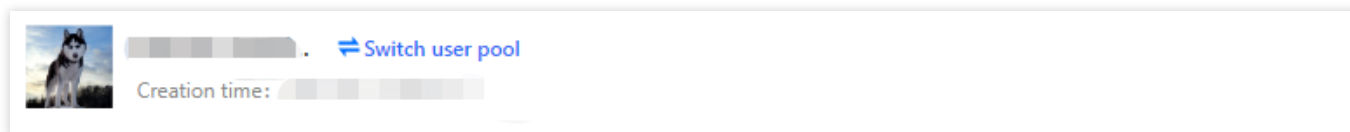
1. Log in to the CIAM console and select **Overview** in the left navigation pane.

2. On the **Overview** page, you can switch pools in the following two ways:

Method 1: Click **Switch user pool** in the upper left corner of the page and select the user pool to switch to.



Method 2: Click **Manage user pool** in the upper right corner of the page to go to the **User pool management details** page. Then, select the user pool to switch to.



# Setting the default user pool

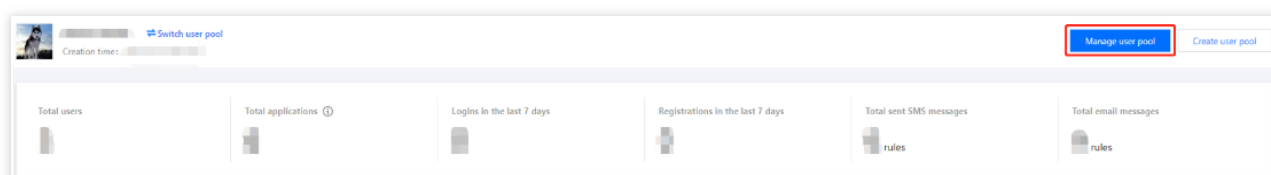
Last updated : 2023-12-22 11:42:07

## Scenarios

Customer Identity and Access Management (CIAM) supports multiple user pools. If an administrator is in charge of managing a certain user pool, the administrator can set it as the default user pool. After the default user pool is set, the user pool is displayed by default each time the administrator logs in.

## Steps

1. Log in to the [CIAM console](#) and select **Overview** in the left navigation pane.
2. On the **Overview** page, Click **Manage user pool** in the upper right corner to go to the **User pool management details** page.

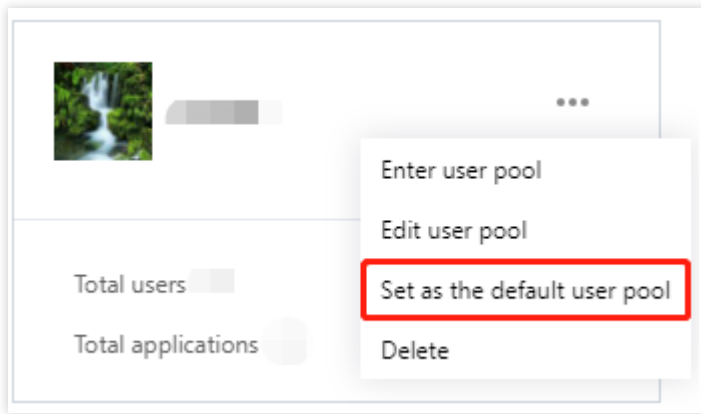


3. On the **User pool management details** page, click

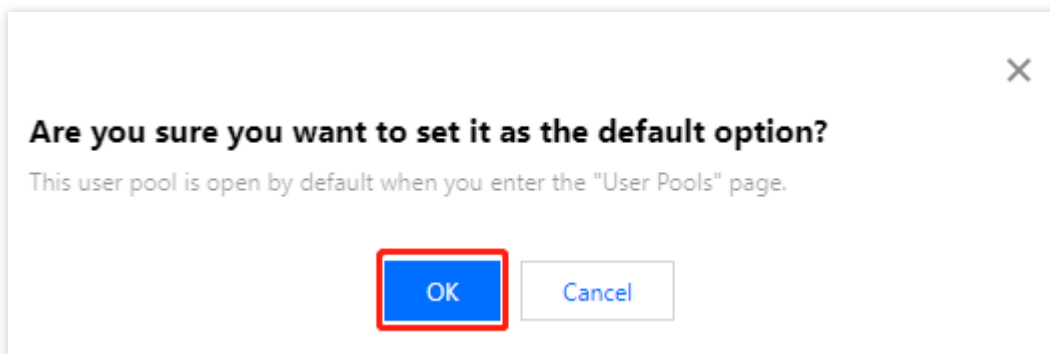


and select **Set as the default user pool**.





4. In the confirmation window displayed, click **OK** to set the default user pool.



# Editing a user pool

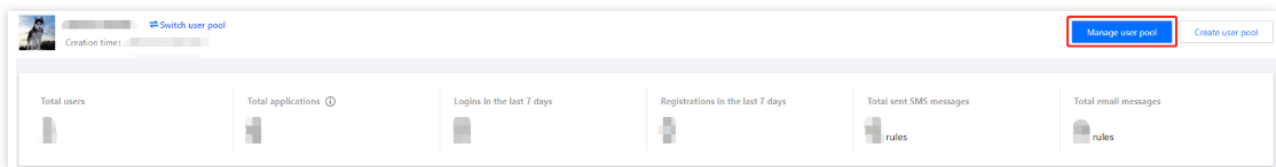
Last updated : 2023-12-22 11:42:08

## Scenarios

After creating a user pool, you can modify its information, such as the user pool name and logo image.

## Steps

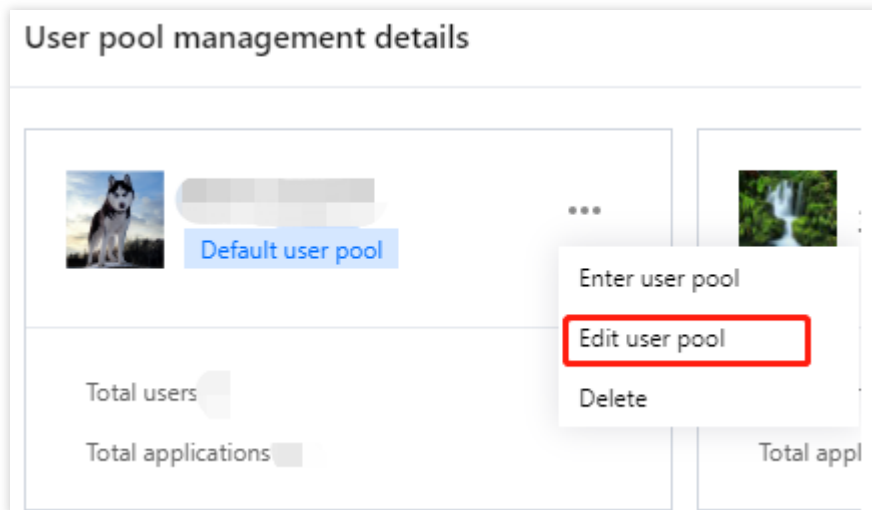
1. Log in to the [Customer Identity and Access Management console](#) and select **Overview** in the left navigation pane.
2. On the **Overview** page, Click **Manage user pool** in the upper right corner to go to the **User pool management details** page.



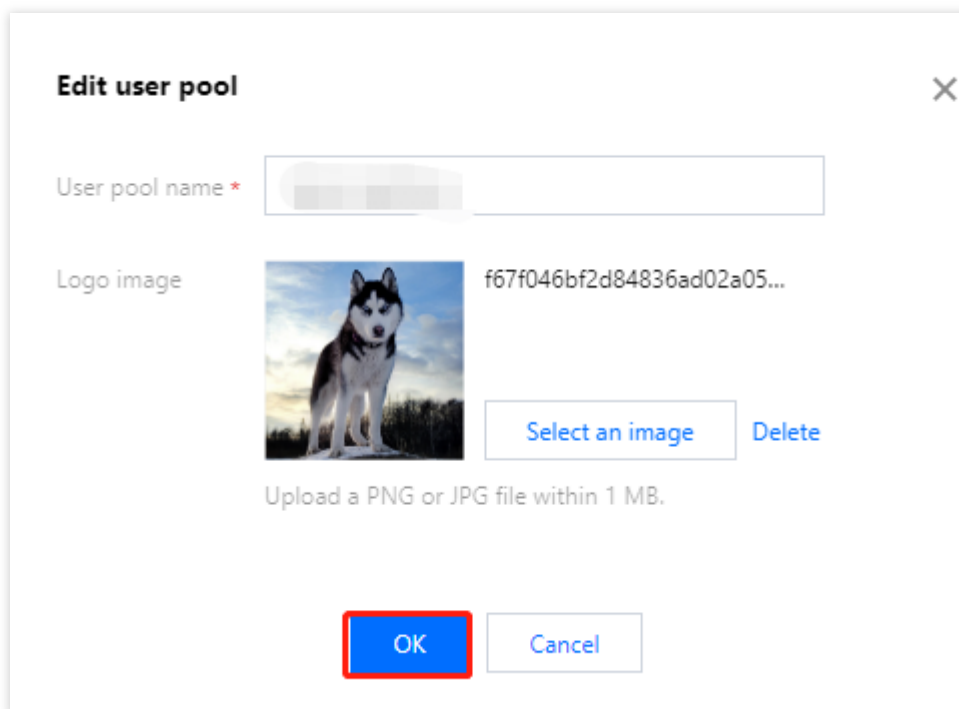
3. On the **User pool management details** page, click



and select **Edit user pool**.



4. In the **Edit user pool** window displayed, edit the user pool information and click **OK**.



**Parameter description:**

User pool name: This field cannot be empty. The name must be unique and cannot exceed 128 characters.

Logo image: Upload a PNG or JPG file within 1 MB.

# Deleting a user pool

Last updated : 2023-12-22 11:42:07

## Scenarios

Customer Identity and Access Management (CIAM) supports multiple user pools. Administrators can delete one or more user pools as needed.

### Note:

Deleting a user pool will delete all data in the user pool, including the data of users, custom attributes, user groups, applications, and authentication sources. Please proceed with caution.

## Prerequisites

Close all open applications before deleting a user pool.

## Steps

1. Log in to the [CIAM console](#) and select **Overview** in the left navigation pane.
2. On the **Overview** page, Click **Manage user pool** in the upper right corner to go to the **User pool management details** page.



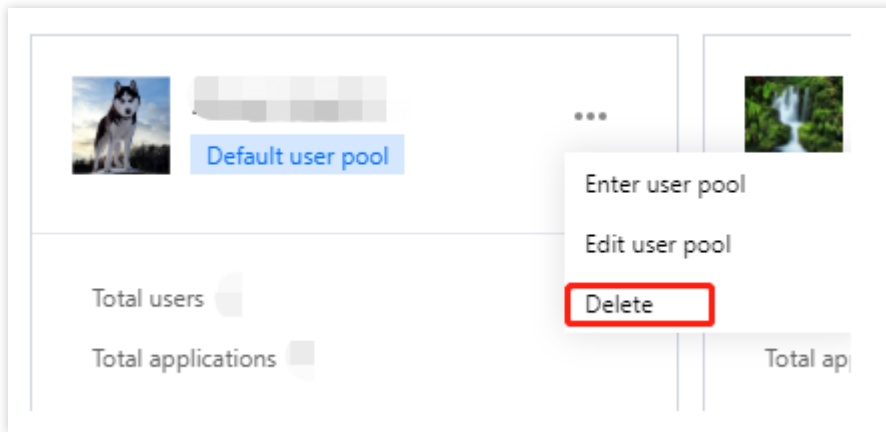
3. On the **User pool management details** page, click



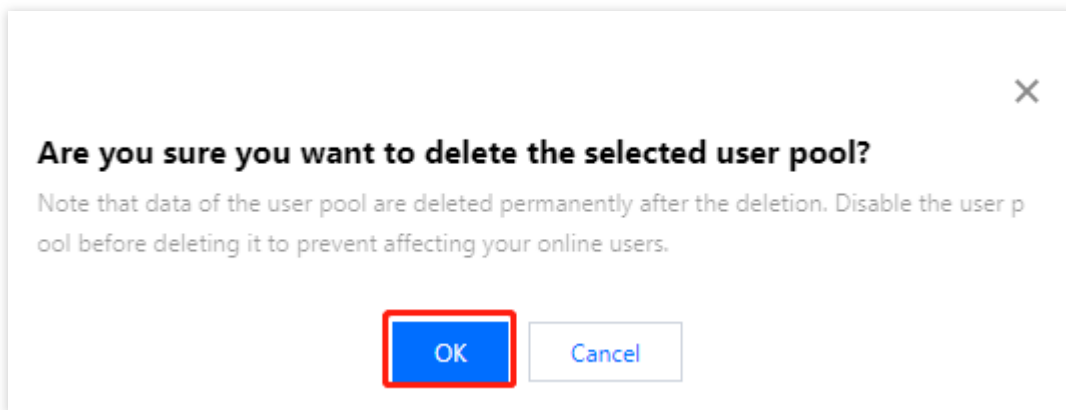
and select **Delete**.

### Note:

If you enabled operation protection in [Security Settings](#) in the **Account Center**, you have to verify your identity before deleting a user pool. After your identity is verified, you do not need to verify your identity again to delete user pools within 30 minutes.



4. In the confirmation window, click **OK**.



# User management

## Custom attributes

### Creating a custom attribute

Last updated : 2023-12-22 11:42:07

## Scenarios

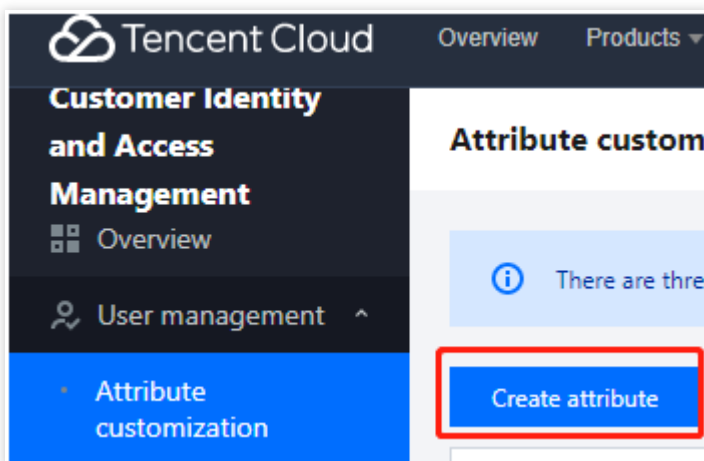
After creating user directories, you can create custom attributes.

### Note:

There are three types of attributes, namely built-in attributes, preset attributes and custom attributes. The built-in attributes cannot be modified/deleted, while the preset attributes and custom attributes can be modified and deleted. Once the end user data is generated, the associated preset attributes and custom attributes cannot be modified.

## Steps

1. Log in to the [Customer Identity and Access Management console](#) and select **User management -> Custom attributes** in the left navigation pane.
2. On the **Custom attributes** page, click **Create attribute**.



3. In the **Create attribute field** window displayed, fill in the basic information and click **OK** to add the attribute. If needed, you can also add a regular expression and an error message for this attribute.

### Create attribute field ✕

\* Attribute name

\* Attribute label

\* Field Type

Data masking rules

**Regex** ▲

Regular Expression

Error

# Editing a custom attribute

Last updated : 2023-12-22 11:42:08

## Scenarios

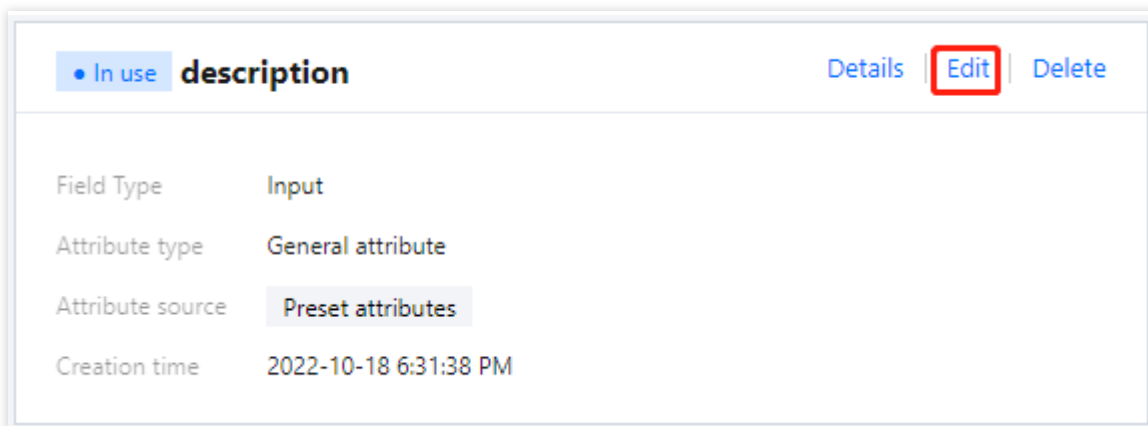
After adding custom attributes, you can modify the attribute information, such as the attributes' fields, regular expressions, and error messages.

### Note:

Built-in attributes cannot be modified. Preset or custom attributes can be modified.

## Steps

1. Log in to the [Customer Identity and Access Management console](#). Select **User management** -> **Custom attributes** in the left navigation pane.
2. On the **Custom attributes** page, click **Edit**.



3. In the **Edit attribute fields** window displayed, edit the attribute information and click **OK**.



### Edit attribute fields ✕

\* Attribute name

\* Attribute label

\* Field Type

Data masking rules

**Regex** ▲

Regular Expression

Error

# Viewing custom attributes

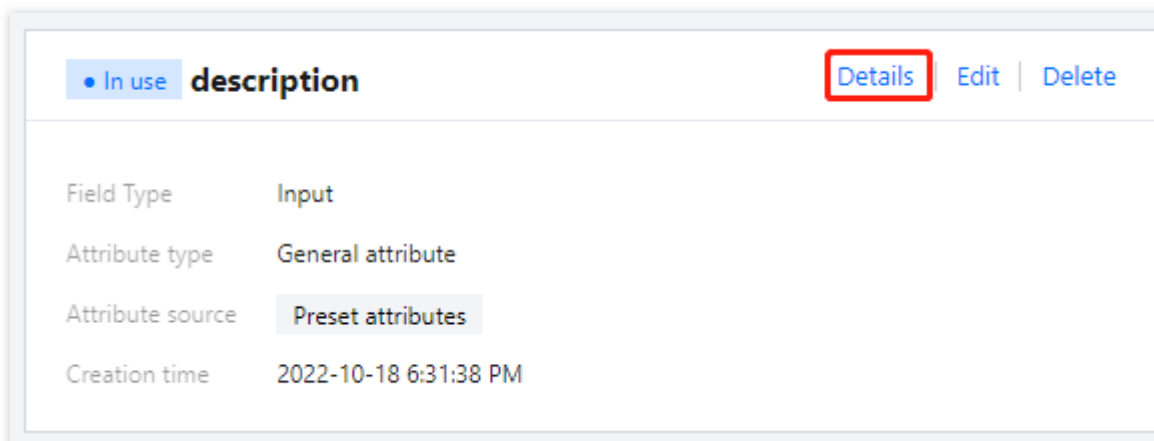
Last updated : 2023-12-22 11:42:07

## Scenarios

After adding custom attributes, you can view the attribute information, such as the attributes' fields, regular expressions, and error messages.



## Steps

1. Log in to the [Customer Identity and Access Management console](#). Select **User management** -> **Custom attributes** in the left navigation pane.
2. On the **Custom attributes** page, click **Details**.



3. In the **Check attribute field details** window displayed, you can view the details of the attribute fields.

### Check attribute field details ✕

Attribute name	description 
In Use	<span>• In use</span>
Field Type	Input
Attribute type	General attribute
Attribute source	<span>Preset attributes</span>
Creation time	2022-10-18 18:31:38
Attribute label	description 
Regular Expression	-
Error	-

# Deleting a custom attribute

Last updated : 2023-12-22 11:42:08

## Scenarios

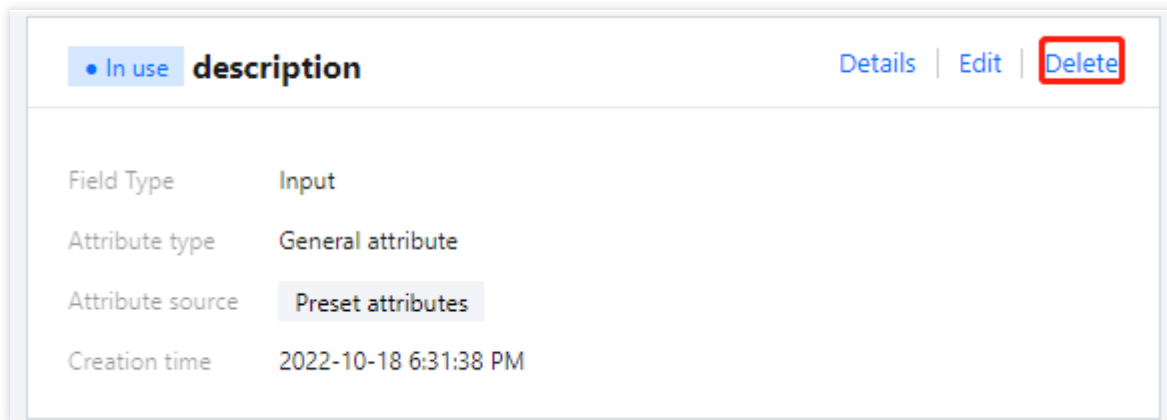
You can delete custom attributes as needed.

### Note:

Built-in attributes cannot be deleted. Preset or custom attributes can be deleted.

## Steps

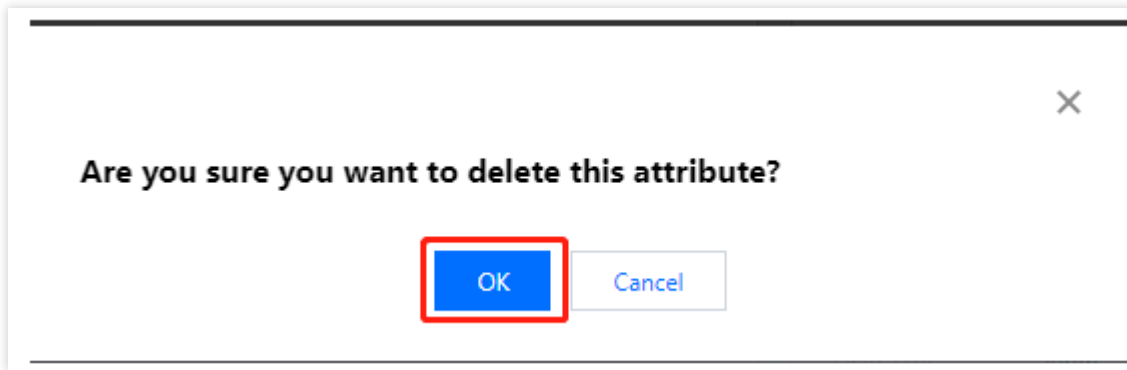
1. Log in to the [Customer Identity and Access Management console](#). Select **User management** -> **Custom attributes** in the left navigation pane.
2. On the **Custom attributes** page, click **Delete**.



3. In the confirmation window displayed, 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.



# Creating a user

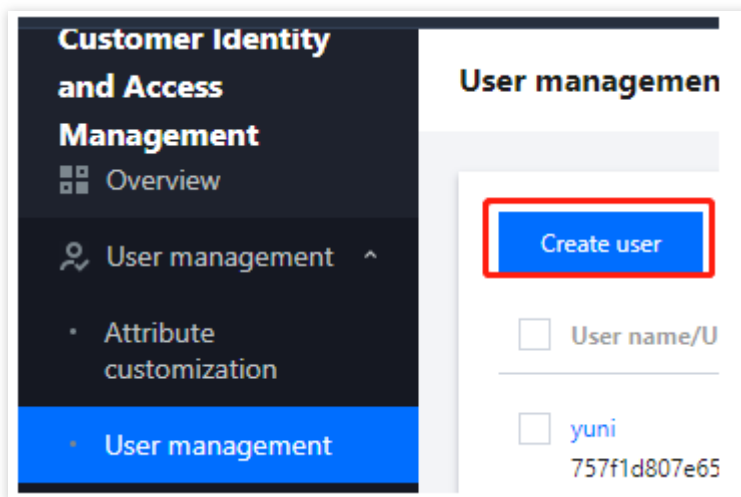
Last updated : 2023-12-22 11:42:07

## Scenarios

After creating user pools and custom attributes, you can create users.

## Steps

1. Log in to the [Customer Identity and Access Management console](#) and select **User management** -> **User management** in the left navigation pane.
2. On the **User management** page, click **Create user**.



3. In the **Create user** window displayed, fill in the basic information and click **OK** to add the user.

### Note:


By default, the new user is in the disabled state. The status of the user changes to enabled after the user logs in.

### Create user ✕

userName \*


nickname

email \*

Password \*  

Phone nu...

userGroup

birthdate  

address

input

phone

emails

# Viewing user details

Last updated : 2023-12-22 11:42:07

## Scenarios

After adding a user, you can view the user details, such as the user's basic information and user group.

## Steps

1. Log in to the [Customer Identity and Access Management console](#) and select **User management** -> **User management** in the left navigation pane.
2. On the **User management** page, click the **username** to go to the user details page.



3. On the user details page, you can view the user's information and user group.





**autotest001**

User status: • Normal

**Basic information**

Customer name	-	Last login	[Redacted]
User ID	[Redacted]	Latest edited	[Redacted]
User group	-	Creation time	[Redacted]

**Details**

userName	[Redacted]	email	[Redacted]
phoneNumber	[Redacted]	wechatUnionId	-
alreadyFirstLogin	[Redacted]	wechatOpenId	-
lockTime	-	source	[Redacted]
errorCount	-	zoneinfo	-
locale	-	alipayUserId	-
qqOpenId	-	qqUnionId	-
residentIdentityC...	-	identityVerificati...	-
name	-	identityVerified	[Redacted]
lockType	-	description	-

# Editing user attributes

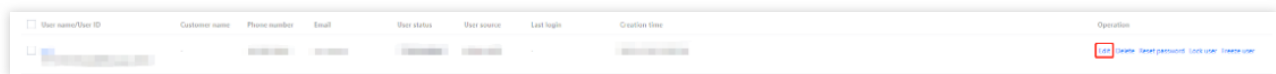
Last updated : 2023-12-22 11:42:07

## Scenarios

After adding a user, you can modify the user attributes, such as the username, associated email address, and mobile number.

## Steps

1. Log in to the [Customer Identity and Access Management console](#) and select **User management** -> **User management** in the left navigation pane.
2. On the **User management** page, click **Edit** in the operation column.



User name/User ID	Customer name	Phone number	Email	User status	User source	Last login	Creation time	Operation
[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	<a href="#">Edit</a> <a href="#">Reset password</a> <a href="#">Link user</a> <a href="#">Invite user</a>

3. In the **Edit user** window displayed, edit the user information and click **OK**.

### Edit user ✕


userName \*

nickname

email \*

Phone nu...

userGroup

birthdate  

address

input

phone

emails

number

# Deleting a user

Last updated : 2023-12-22 11:42:07

## Scenarios

After adding users, you can delete one or more users as needed.

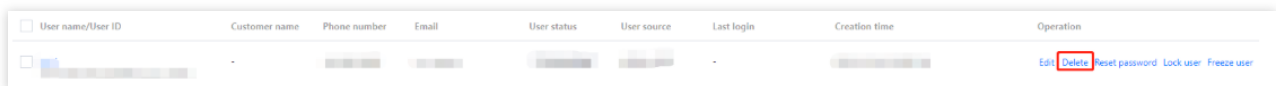
### Note:

All the data of deleted users cannot be recovered. Please proceed with caution.

## Steps

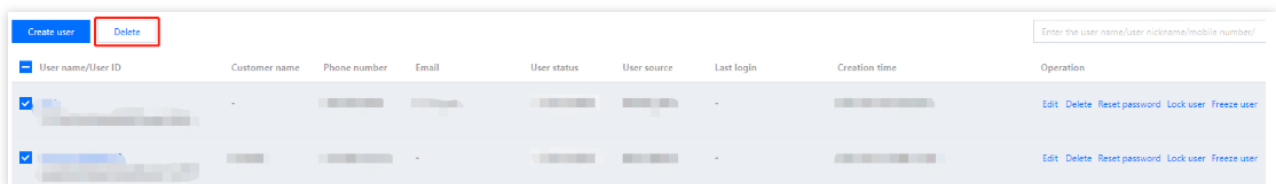
1. Log in to the [Customer Identity and Access Management console](#) and select **User management -> User management** in the left navigation pane.
2. On the **User management** page, you can delete one or more users.

Deleting a single user: Select the user to delete and click **Delete** in the operation column.



<input type="checkbox"/>	User name/User ID	Customer name	Phone number	Email	User status	User source	Last login	Creation time	Operation
<input checked="" type="checkbox"/>	[blurred]	-	[blurred]	[blurred]	[blurred]	[blurred]	-	[blurred]	Edit <b>Delete</b> Reset password Lock user Freeze user

Deleting multiple users: Select one or more users to delete and click **Delete** at the top of the list.



<input type="checkbox"/>	User name/User ID	Customer name	Phone number	Email	User status	User source	Last login	Creation time	Operation
<input checked="" type="checkbox"/>	[blurred]	-	[blurred]	[blurred]	[blurred]	[blurred]	-	[blurred]	Edit Delete Reset password Lock user Freeze user
<input checked="" type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	-	[blurred]	Edit Delete Reset password Lock user Freeze user

3. In the confirmation window displayed, click **OK** to delete the selected user(s).

×

**Are you sure you want to delete the selected user(s)?**

You've selected 2 item(s). [Show details](#) ▾

When the selected users are deleted, all related data is cleared and cannot be restored.

OKCancel

# Resetting a password

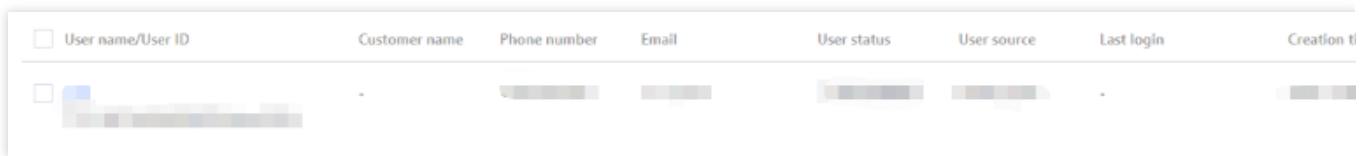
Last updated : 2023-12-22 11:42:07

## Scenarios

If a user forgets their password or a user is locked after too many failed login attempts, administrators can reset the user's password.

## Steps

1. Log in to the [Customer Identity and Access Management console](#) and select **User management** -> **User management** in the left navigation pane.
2. On the **User management** page, click **Reset password** in the operation column.

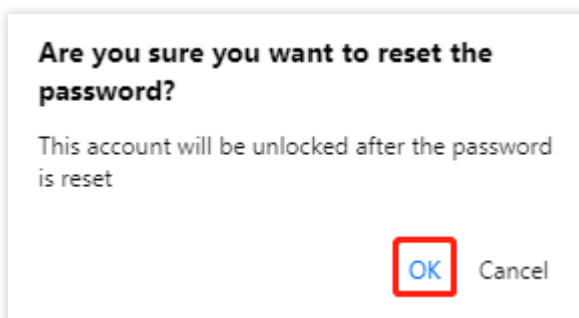


<input type="checkbox"/>	User name/User ID	Customer name	Phone number	Email	User status	User source	Last login	Creation ti
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]

3. In the confirmation window displayed, click **OK** to reset the password.

### Note:

This account will be unlocked after the password is reset.



# Freezing or locking users

Last updated : 2023-12-22 11:42:08

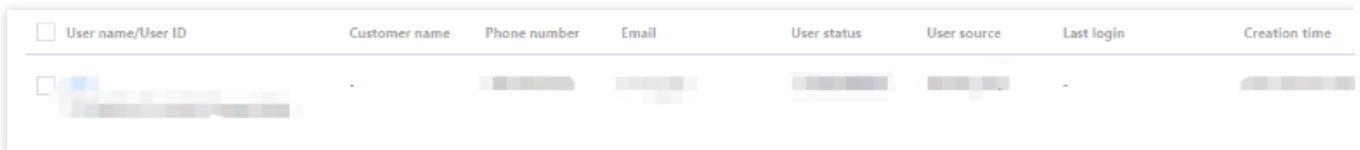
## Scenarios

After adding users, you can lock or freeze a user to block the user from logging in to the Customer Identity and Access Management (CIAM) console.

## Steps

### Locking a user

1. Log in to the [CIAM console](#) and select **User management** -> **User management** in the left navigation pane.
2. On the **User management** page, click **Lock user** in the operation column.



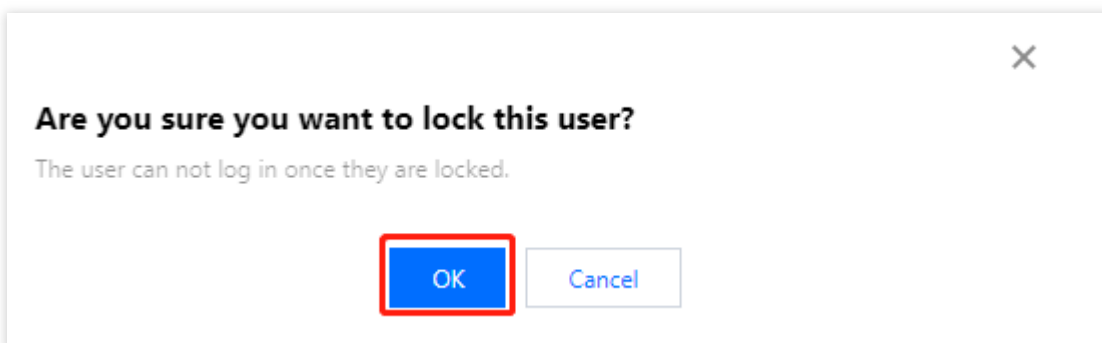
<input type="checkbox"/>	User name/User ID	Customer name	Phone number	Email	User status	User source	Last login	Creation time
<input checked="" type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]

3. In the confirmation window displayed, click **OK** to lock the user. Then, the user cannot log in to the console.

### Note:

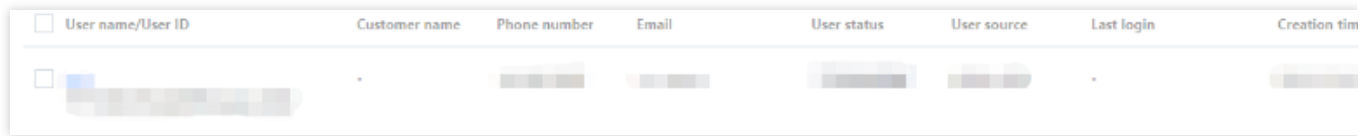
If a user is locked by an administrator, the user can be unlocked only by an administrator.

If a user is locked after too many failed login attempts, the user will be automatically unlocked according to the unlock policy.



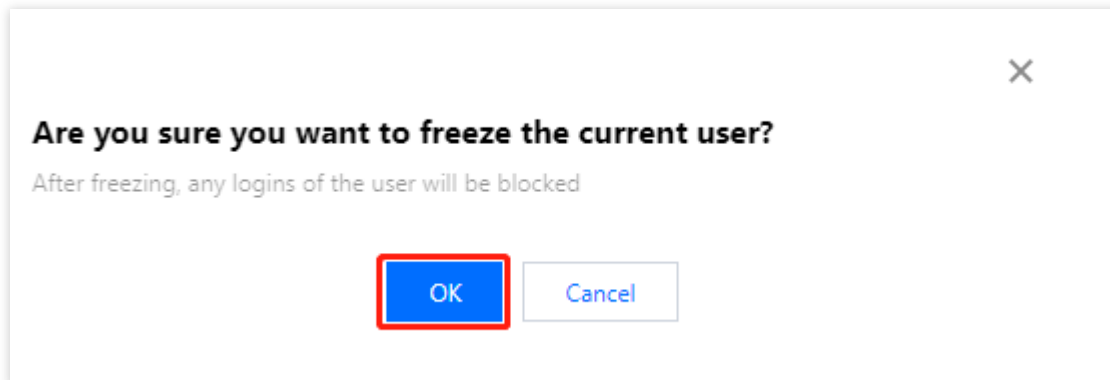
### Freezing a user

1. Log in to the [CIAM console](#) and select **User management** -> **User management** in the left navigation pane.
2. On the **User management** page, click **Freeze user** in the operation column.



<input type="checkbox"/>	User name/User ID	Customer name	Phone number	Email	User status	User source	Last login	Creation time
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]

3. In the confirmation window displayed, click **OK** to freeze the user. Then, the user cannot log in to the console.





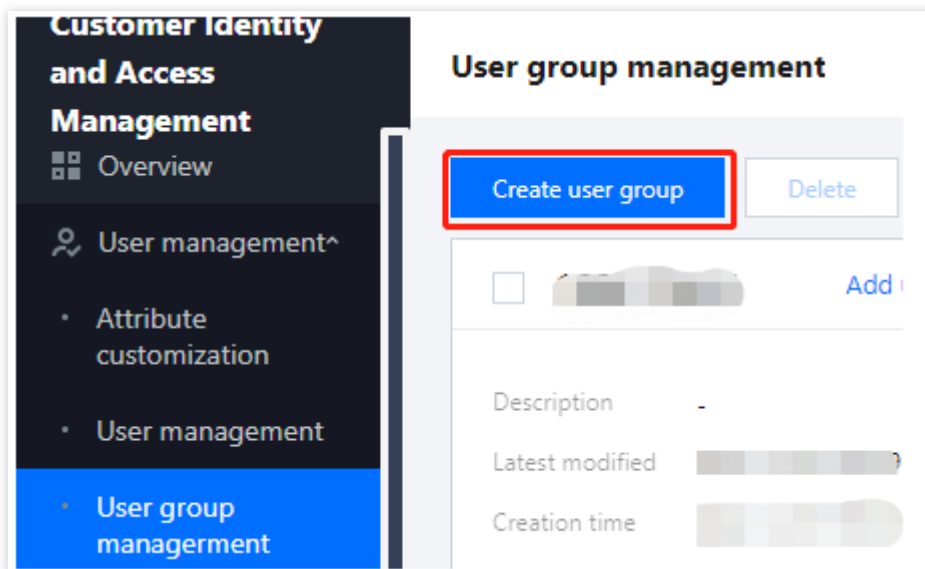
# User group management

Last updated : 2023-12-22 11:42:07

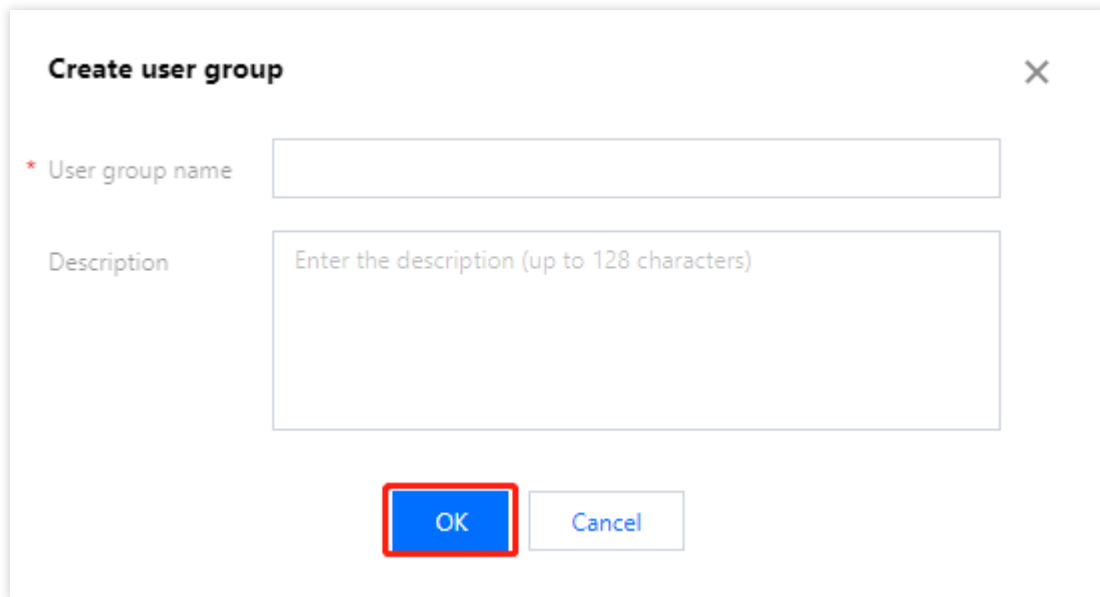
This topic describes how to create or edit a user group and add or remove users from a user group in the Customer Identity and Access Management (CIAM) console.

## Creating a user group

1. Log in to the [CIAM console](#) and select **User group management** in the left navigation pane.
2. On the **User group management** page, click **Create user group**.



3. In the **Create user group** window displayed, enter a user group name and description, and then click **OK** to create the user group.



The image shows a 'Create user group' dialog box. It has a title bar with a close button (X). Below the title bar, there are two input fields: 'User group name' (marked with a red asterisk) and 'Description' (with a placeholder text 'Enter the description (up to 128 characters)'). At the bottom of the dialog, there are two buttons: 'OK' (highlighted with a red border) and 'Cancel'.

**Parameter description:**

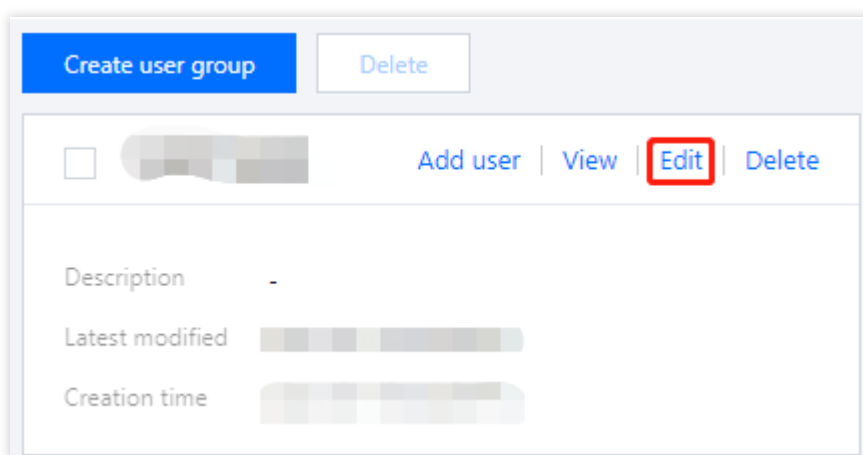
User group name: A unique custom name.

Description: A custom description of up to 128 characters.

## Editing a user group

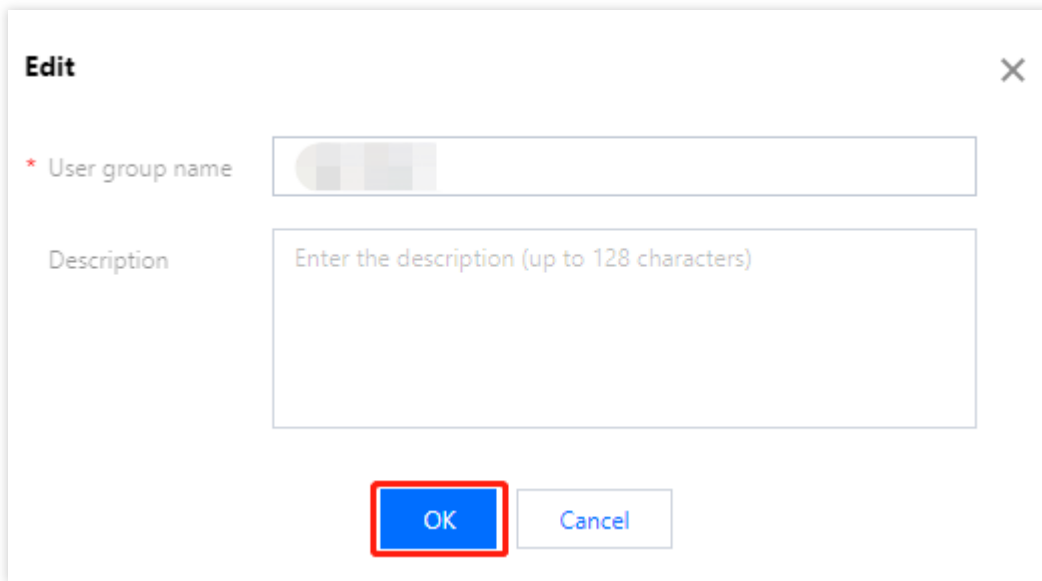
After adding a user group, you can modify the user group name and description.

1. On the [User group management](#) page, select the user group to edit and click **Edit**.



The image shows a table with one row representing a user group. The table has a header row with buttons: 'Create user group' (blue), 'Delete' (white), and a row of actions: 'Add user' (blue), 'View' (blue), 'Edit' (blue, highlighted with a red border), and 'Delete' (blue). Below the header, the table row shows a checkbox, a blurred user group name, and three rows of metadata: 'Description' (with a dash), 'Latest modified' (with a blurred date), and 'Creation time' (with a blurred date).

2. In the **Edit** window displayed, modify the user group name and description, and then click **OK**.



**Edit** ✕

\* User group name

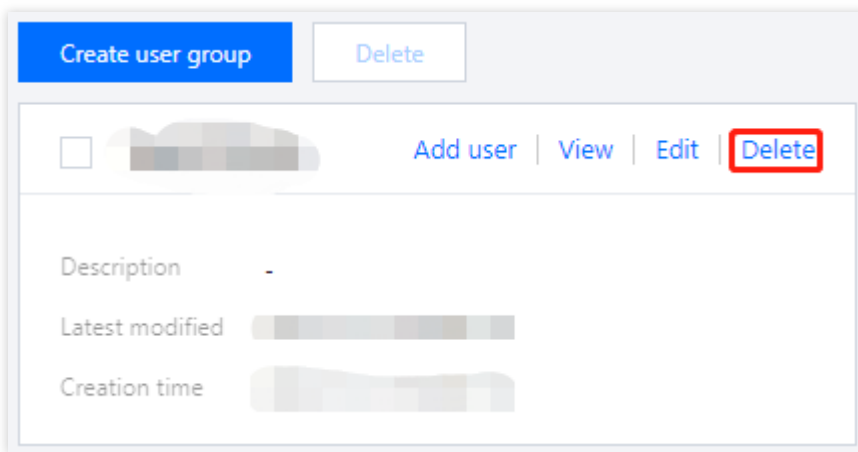
Description

**OK** Cancel

## Deleting a user group

After adding user groups, you can delete one or more user groups as needed on the [User group management](#) page.

Method 1: Select the user group to delete, click **Delete**, and then confirm the deletion.



Create user group Delete

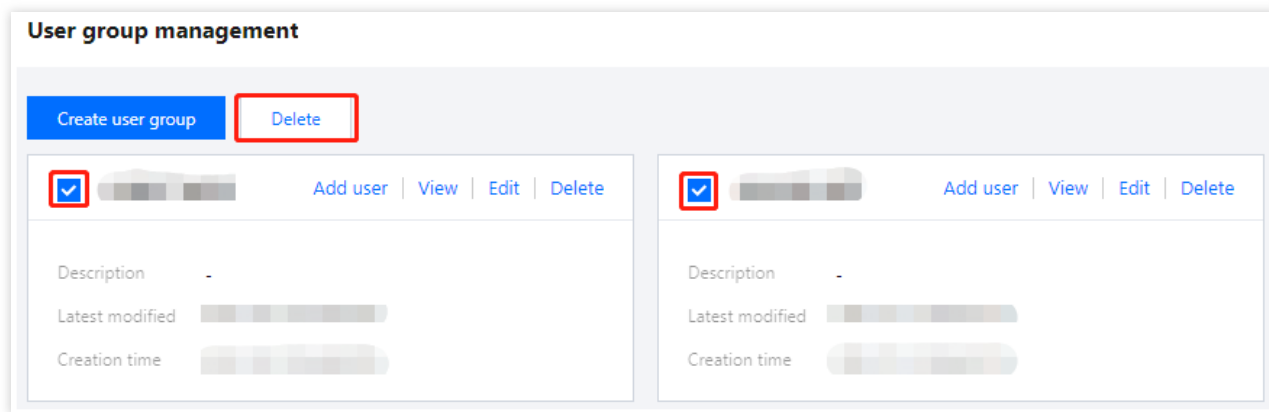
<input type="checkbox"/>		Add user   View   Edit   <b>Delete</b>
--------------------------	--	--

Description -

Latest modified

Creation time

Method 2: Select one or more user groups to delete, click **Delete** at the top of the list, and then confirm the deletion.

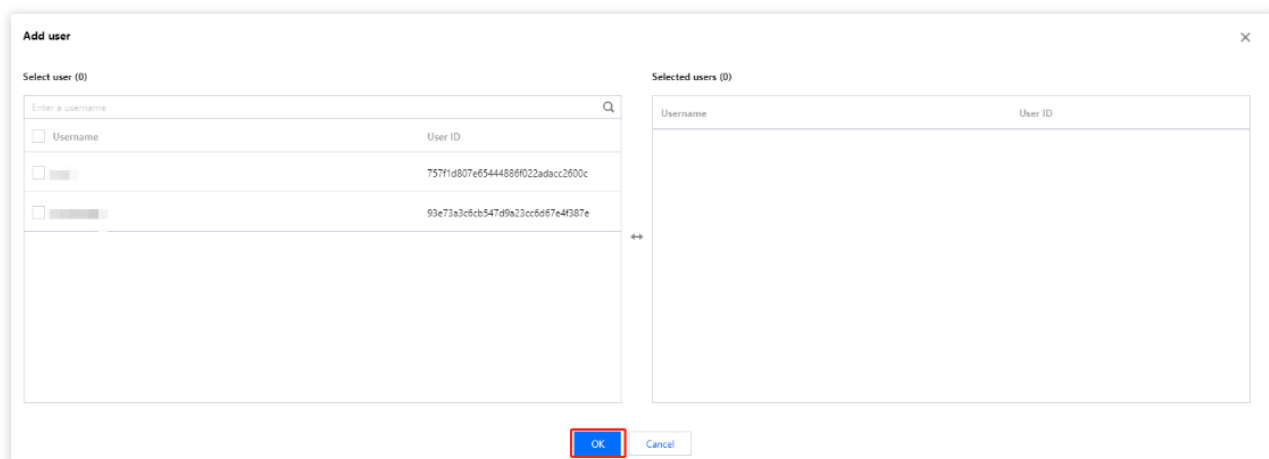


## Adding users to a user group

After creating a user group, you can add users to the user group.

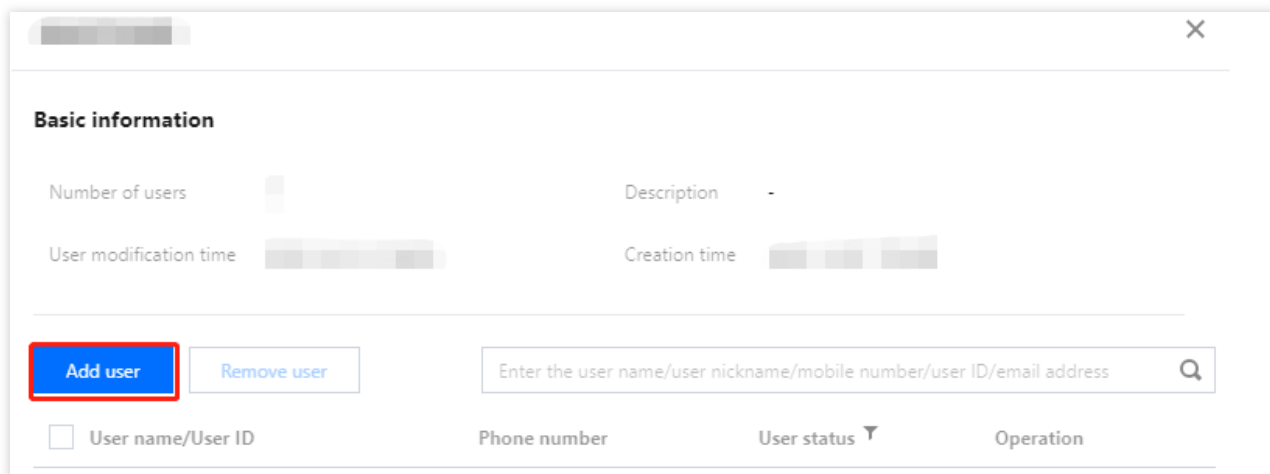
### Method 1

1. On the [User group management](#) page, select the user group you want and click **Add user**.
2. In the **Add user** window displayed, select one or more users to add and click **OK**. Then, the selected users will be added to the user group.

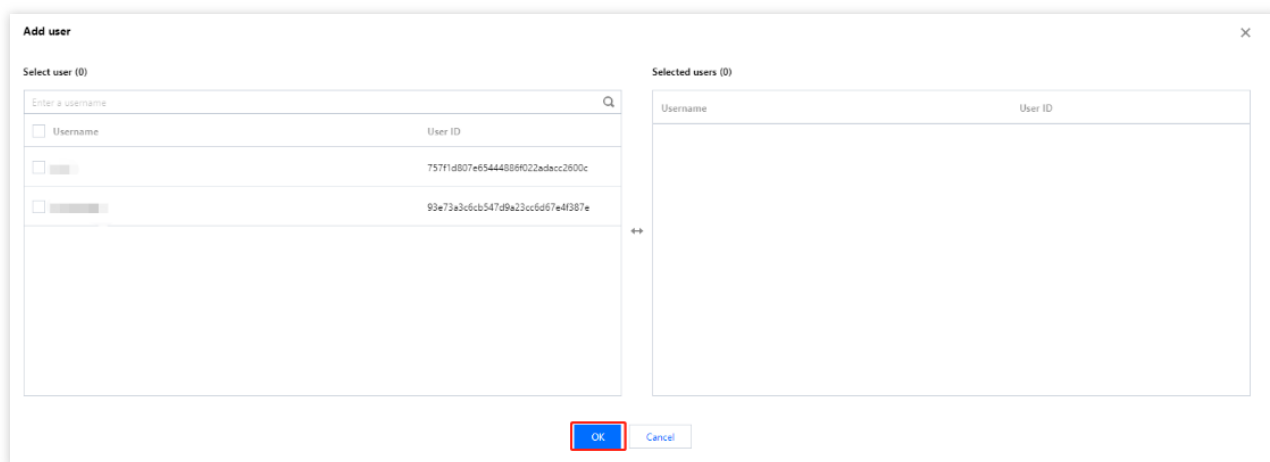


### Method 2

1. On the [User group management](#) page, select the user group you want and click the blank space on the user group.
2. On the **User group details** page, click **Add user**.



3. In the **Add user** window displayed, select one or more users to add and click **OK**. Then, the selected users will be added to the user group.

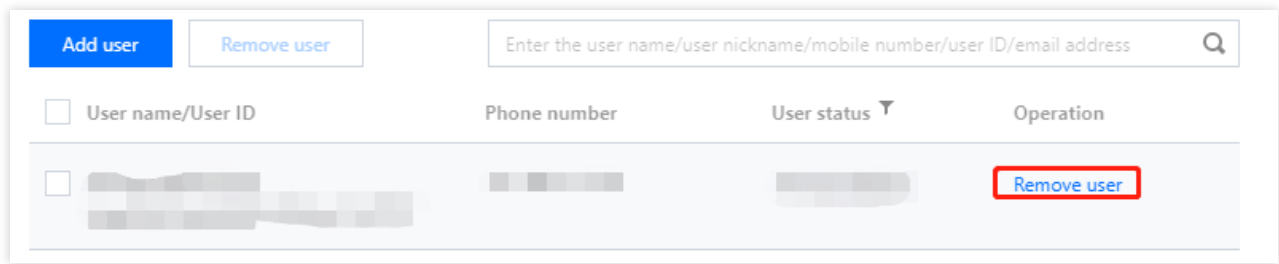


## Removing users from a user group

You can remove users who have been added to a user group.

### Method 1

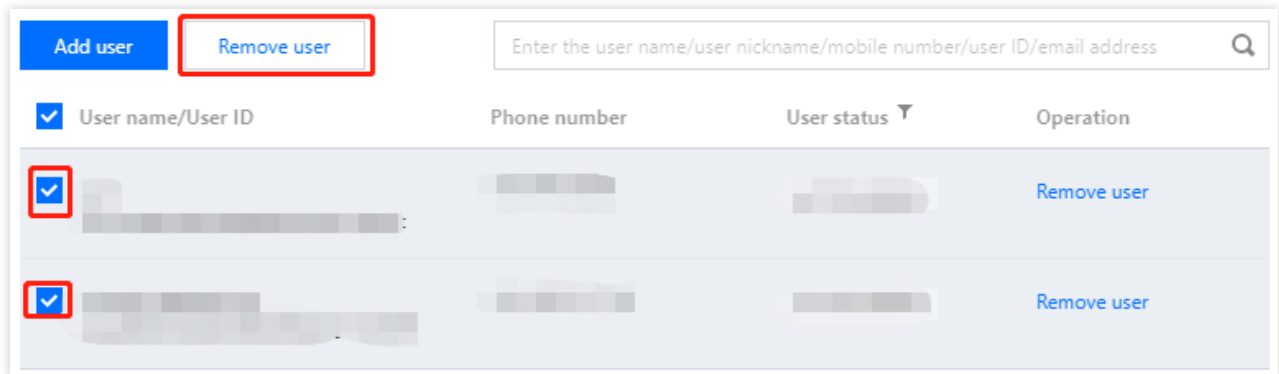
1. On the [User group management](#) page, select the user group you want and click the blank space on the user group.
2. On the **User group details** page, click **Remove user** in the operation column.



3. In the confirmation window displayed, click **OK** to remove the user from the user group.

## Method 2

1. On the [User group management](#) page, select the user group you want and click the blank space on the user group.
2. On the **User group details** page, select one or more users to remove and click **Remove user** at the top of the list.



# Application management

## Creating an application

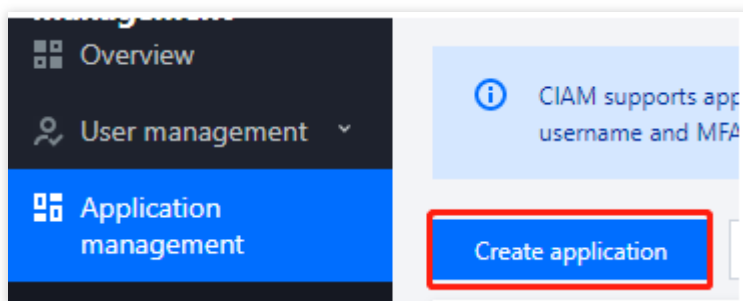
Last updated : 2023-12-22 11:42:07

### Scenarios

Customer Identity and Access Management (CIAM) allows administrators to create external-facing business applications, including Web applications, mobile apps, one-page applications, WeChat Mini Programs, and M2M applications. An administrator must create an application before configuring the parameters and processes such as registration or login.

### Steps

1. Log in to the [CIAM console](#) and select **Application management** in the left navigation pane.
2. On the **Application management** page, click **Create application** at the top of the list.




3. In the **Create application** window displayed, fill in the required information and click **OK** to create the application.

#### Note:

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

### Create application ✕

Application icon \*      application\_default.svg



[Select an image](#)   [Delete](#)

Upload a PNG or JPG file within 1 MB.

Template Name \*   

Application type \*   

Industry

Description

- One-page application
- Mobile App
- Web application
- WeChat Mini Program application
- M2M application

[OK](#)   [Cancel](#)



# Configuring an application


Last updated : 2023-12-22 11:42:07

## Scenarios

Customer Identity and Access Management (CIAM) allows administrators to configure created applications as needed, including the basic information (such as the icon and name), the parameters (such as the redirect and logout addresses), and the processes (such as registration, login, password reset, and protocol management).

## Steps

1. Log in to the [CIAM console](#) and select **Application management** in the left navigation pane.
2. On the **Application management** page, click **Configuration** in the operation column.

<input type="checkbox"/>	Application name/Client ID	Application type <span>▾</span>
<input type="checkbox"/>	 <b>Web1313123121</b> MTZiYjiMjBIZTMzNGYwYThkMjA3NmUyOGQwNjcxNDM	Web application

## Basic information

The screenshot displays the 'Basic information' tab of an application configuration page. The page has four tabs: 'Basic information', 'Parameter configuration', 'Process configuration', and 'CORS'. The 'Basic information' tab is active. The form contains the following fields:

- Application icon \***: A placeholder image with a blue cube icon. Below it are buttons for 'Select an image' and 'Delete'. A note below the buttons says 'Upload a PNG or JPG file within 1 MB.'
- Template Name \***: A text input field.
- Application type \***: A dropdown menu currently set to 'Web application'.
- Industry**: A text input field.
- Client ID**: A text input field.
- Secret**: A text input field.
- Description**: A text area.

At the bottom left, there are two buttons: 'OK' (highlighted with a red box) and 'Cancel'.

## Parameter configuration

1. On the **Application configuration** page, click the **Parameter configuration** tab.
2. On the **Parameter configuration** tab, fill in the required information and click **OK** to save the configuration.

Redirect URI + Add  
 Enter the complete URI addresses starting with the protocol (for example https://example.c

Logout Redirect URI + Add  
 Enter the complete URI address starting with the protocol (for example https://example.cor

Access\_token validity \* - 600 + seconds

refresh\_token  Enable refresh\_token

Claims Enter the authentication source attribute

---

OK
Cancel

Parameter description:

Parameter	Description	Example
Redirect URI	A complete URL starting with http or https for receiving the OAuth authorization code. After the user authorizes the request, this code will be redirected to the address.	<a href="https://www.qq.com">https://www.qq.com</a>
Logout Redirect URI	A complete URL starting with http or https, to which the user will be redirected after logout.	https://www.qq.com/logout
Access_token validity	The validity period of access tokens. The default validity is 600 seconds.	600
refresh_token	Specifies whether refresh tokens are enabled.	-
Refresh_token validity period	The validity period of refresh tokens. This parameter is displayed when refresh tokens are enabled. The default validity is 86,400 seconds.	86400

### Process configuration

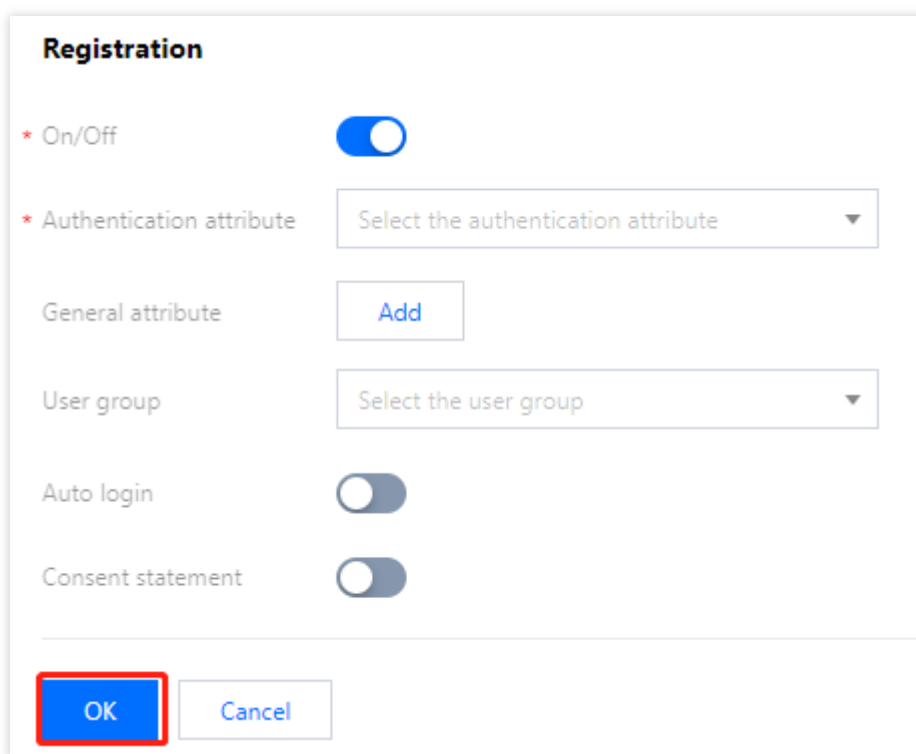
You can configure the registration, login, MFA, username retrieval, and password reset processes. By configuring different parameters, you can customize the registration, login, and other processes for applications.

For Web applications, one-page applications, and mobile apps, you can configure the registration, login, MFA, username retrieval, and password reset processes.

### Configuring Web applications, one-page applications, and mobile apps

1. On the **Application configuration** page, click the **Process configuration** tab.
2. The **Process configuration** tab contains five modules for the registration, login, MFA, username retrieval, and password reset processes.

**Registration:** Click **Edit** in the upper right corner of the module to configure the parameters, and then click **OK** to save the configuration.



**Registration**

\* On/Off

\* Authentication attribute

General attribute

User group

Auto login

Consent statement

#### Parameter description:

**On/Off:** By default, the toggle is turned on. Users cannot register for the application if the toggle is turned off.

**Authentication attribute:** This field is filled in by users during registration. It can be used as a unique user identifier.

**SMS OTP authentication source:** The policy for sending SMS OTPs during registration. This field must be configured if you select the phone number as the authentication attribute.

**Email OTP authentication source:** The policy for sending email OTPs during registration. This field must be configured if you select the email address as the authentication attribute.

**General attribute:** This field is filled in by users during registration. It cannot be used as a unique user identifier.

**User group:** The group to which users belong after successful registration.

**Auto login:** If the toggle is turned on, users are automatically logged in to the application after successful registration. If the toggle is turned off, users are redirected to the login page after successful registration and need to log in.

Consent statement: If the toggle is turned on, you can configure the consent statement displayed on the registration page as instructed below.

### Instructions

Input format Text + Markdown hyperlink

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

Samples

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

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

### Login

\* On/Off

\* Preferred authentication source

Associate authentication source

Remember password

Consent statement

**Parameter description:**

**On/Off:** By default, the toggle is turned on. Users cannot log in to the application if the toggle is turned off.

**Preferred authentication source:** The preferred authentication method displayed on the login page.

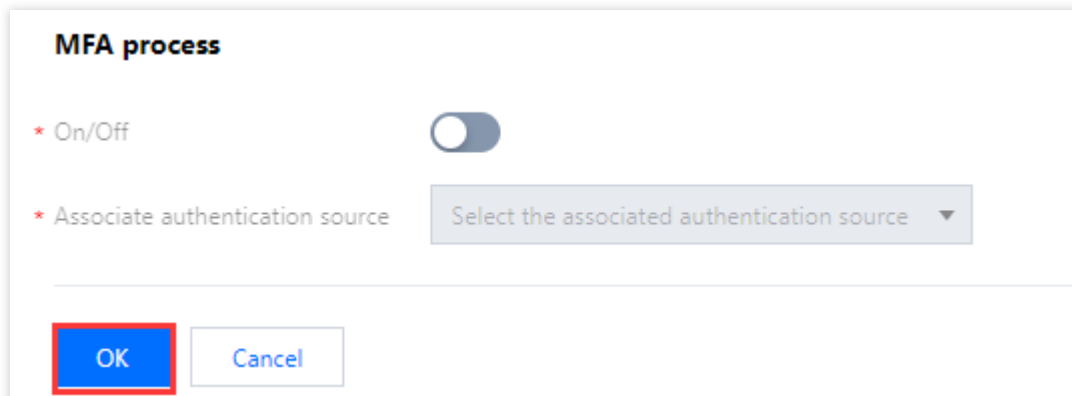
**Associate authentication source:** The alternative authentication method displayed on the login page.

**claims:** The obtained token and the user attribute field returned by the DescribeUserInfo API.

**Remember password:** Specifies whether the browser remembers the password.

**Consent statement:** If the toggle is turned on, you can configure the consent statement displayed on the login page.

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



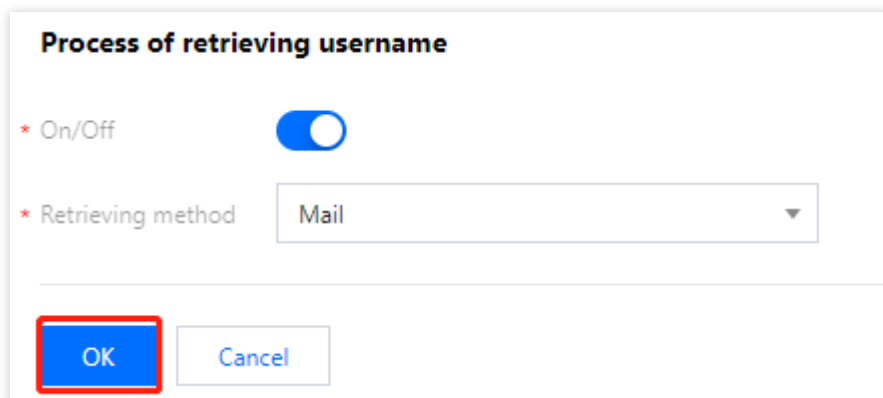
The screenshot shows a configuration dialog box titled "MFA process". It contains two main settings: "On/Off" with a toggle switch currently turned off, and "Associate authentication source" with a dropdown menu showing "Select the associated authentication source". At the bottom, there are two buttons: "OK" (highlighted with a red border) and "Cancel".

**Parameter description:**

On/Off: By default, the toggle is turned off. If the toggle is turned on, 2FA will be enabled.

Associate authentication source: The authentication method. The valid values include SMS OTP and email OTP authentication sources.

**Process of retrieving username:** Click **Edit** in the upper right corner of the module to configure the parameters, and then click **OK** to save the configuration.



The screenshot shows a configuration dialog box titled "Process of retrieving username". It contains two main settings: "On/Off" with a toggle switch currently turned on, and "Retrieving method" with a dropdown menu showing "Mail". At the bottom, there are two buttons: "OK" (highlighted with a red border) and "Cancel".

**Parameter description:**

On/Off: By default, the toggle is turned on. Users cannot retrieve their usernames if the toggle is turned off.

Retrieving method: The method of receiving usernames, such as email.

**Process of resetting password:** Click **Edit** in the upper right corner of the module to configure the parameters, and then click **OK** to save the configuration.

### Process of resetting password

\* On/Off

\* Retrieving method

#### Parameter description:

On/Off: By default, the toggle is turned on. Users cannot reset their passwords if the toggle is turned off.

Retrieving method: The method of receiving verification codes to reset passwords, such as email.

## CORS

To call CIAM APIs by using JavaScript, you need to configure trusted CORS security domains. Up to 10 security domains are allowed.

1. On the **Application configuration** page, click **CORS** to go to the **CORS configuration** page.
2. On the **CORS configuration** page, click **Edit**.

### CORS configuration

CORS -

3. Fill in the required information and click **OK** to save the configuration.

### CORS configuration

CORS

## Notes

The redirect URI of the application is added to the CORS security domain by default. You do not need to configure it here.

Format of CORS: "://" [":"]. For example, `https://sample.portal.tencentciam.com` or

`http://127.0.0.1:8080` . Note that it must start with `https://` or `http://`, and cannot include the request path.

The domain name can only contain [a-z], [0-9] and [.-]. *"-" cannot be used at the beginning or end of the domain name, and it cannot be used consecutively. The wildcard (\*) is only allowed in the first part of the domain name, e.g.*

`https://*.example.com` .



# Authentication management

## General authentication sources

### Creating an authentication source

## Username-password authentication

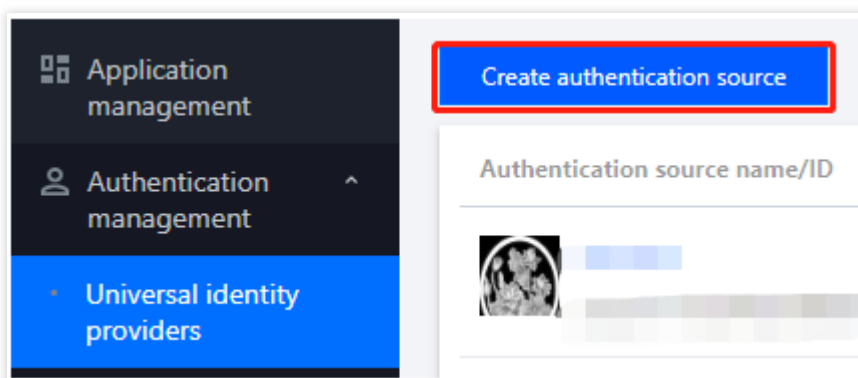
Last updated : 2023-12-22 11:42:07

## Scenarios

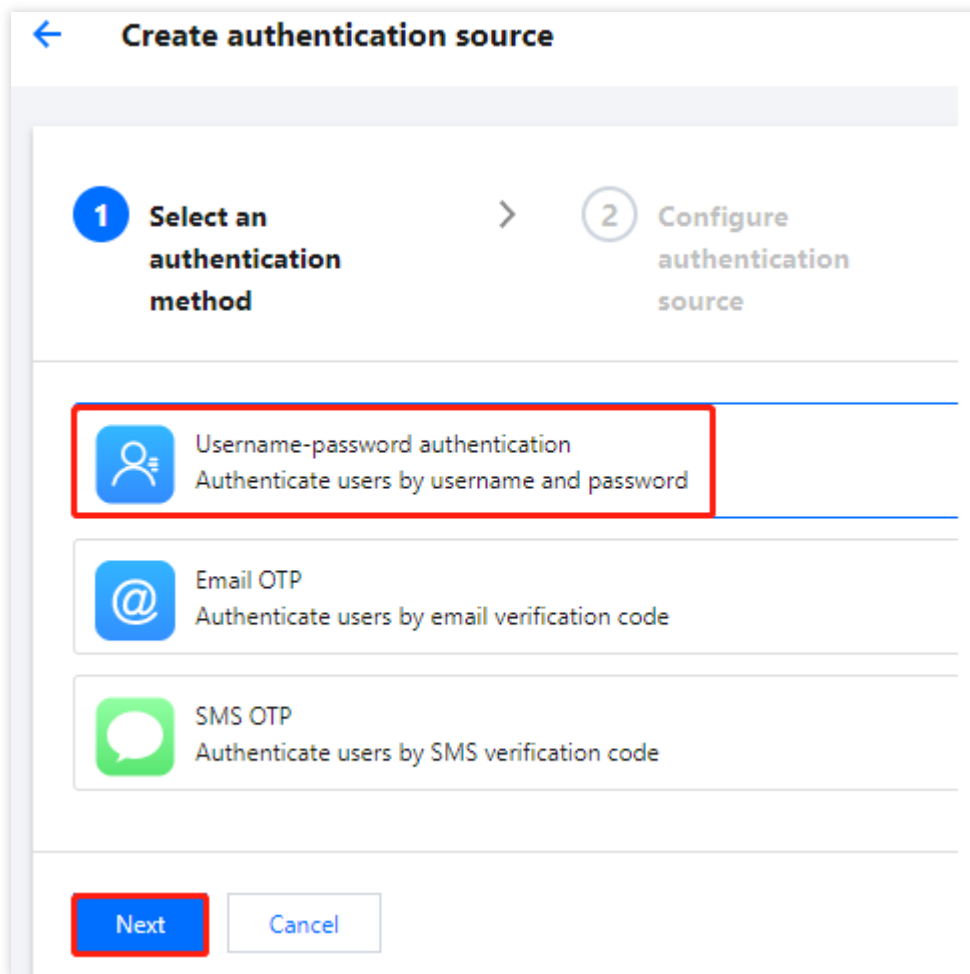
Customer Identity and Access Management (CIAM) supports authenticating users with their usernames and passwords.

## Steps

1. Log in to the [CIAM console](#) and select **Authentication management** -> **General authentication source** in the left navigation pane.
2. On the **General authentication source** page, click **Create authentication source**.



3. On the **Create authentication source** page, select **Username-password authentication** and click **Next**.



4. On the **Create authentication source** page, configure the icon, name, attribute, and description of the authentication source, and then click **Next**.

**Note:**

Authentication source icon: The icon displayed in lists and portals. Click **Upload again** to change the default icon.

Authentication source name: A name to identify the authentication source.


Authentication source attribute: The user attribute used to verify the identities of users during username-password authentication.

Authentication source description: A brief description of the authentication source.

← **Create authentication source**

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

Authentication source icon \* auth\_accountpassword...



Upload a PNG or JPG file within 1 MB.

Authentication source name \*

Authentication source attribute \*

Authentication source description

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

## Policy configuration parameter description

### Configure password policy

Select password policy: Specifies the required strength of passwords set by users. 5 password policies are supported. By default, the required strength is strong.

Password history: Historical passwords. Do not use passwords repeatedly in a short period. The valid range of values is 1-128.

### Password lock

Password lock: If the password lock is enabled, the number of failed login attempts will be restricted.

Lockout threshold: This field is required if the password lock is enabled. If a user's failed login attempts exceed the specified limit, the user is locked and cannot log in until they are unlocked. The valid range of values is 1-999.

Retry period: This field is required if the password lock is enabled. If a user exceeds the lockout threshold within the specified period, the user is locked. The valid range of values is 1-99,999 hours.

Auto-unlock time: This field is required if the password lock is enabled. The time to wait before a locked user is unlocked. The valid range of values is 1-999,999 minutes.

### Verification code

Verification code: If verification codes are enabled, when a user exceeds the maximum number of consecutive failed login attempts, verification code-based verification will be automatically enabled.

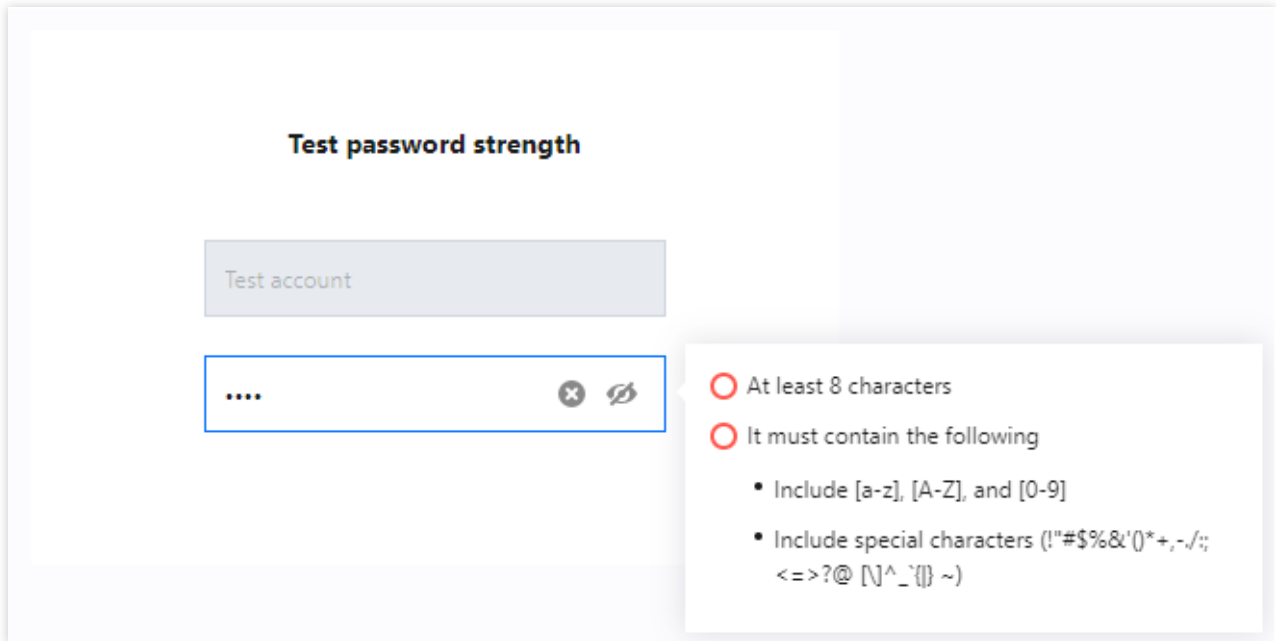
Max attempts: This field is required when verification codes are enabled. If a user's failed login attempts exceed the specified limit, verification code-based verification will be enabled for login. The valid range of values is 1-999.

**Note:**

If the password lock is enabled at the same time, we recommend that you set this field to a value smaller than the lockout threshold. Otherwise, a user may be locked before a verification code is triggered.

**Test password strength**

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



# SMS OTP

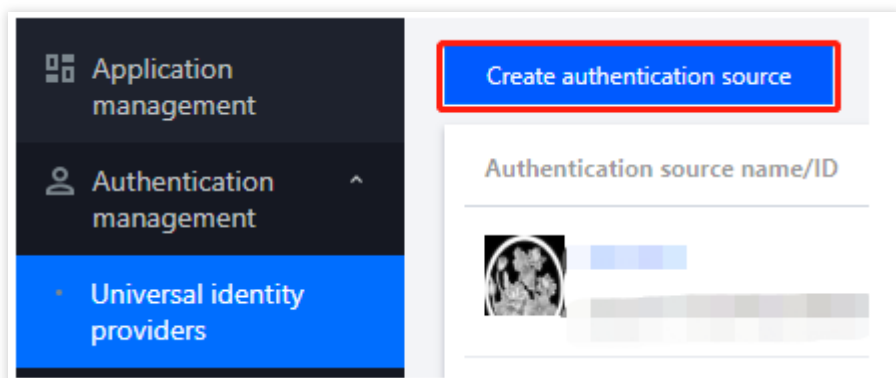
Last updated : 2023-12-22 11:42:07

## Scenarios

Customer Identity and Access Management (CIAM) supports the SMS OTP authentication source. That is, the system authenticates a user by sending an OTP to the mobile number of the user.

## Steps

1. Log in to the [CIAM console](#) and select **Authentication management** -> **General authentication source** in the left navigation pane.
2. On the **General authentication source** page, click **Create authentication source**.



3. On the **Create authentication source** page, select **SMS OTP** and click **Next**.
4. On the **Create authentication source** page, configure the icon, name, attribute, and description of the authentication source, and then click **Next**.

### Note:

Authentication source icon: The icon displayed in lists and portals. Click **Upload again** to change the default icon.

Authentication source name: A name to identify the authentication source.

Authentication source attribute: The SMS OTP authentication source uses the phone number attribute by default. This field cannot be modified.


Authentication source description: A brief description of the authentication source.

### ← Create authentication source

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

---

Authentication source icon \* auth\_message.svg



Upload a PNG or JPG file within 1 MB.

Authentication source name \*

Authentication source attribute \*

Authentication source description

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

**Note:**

Length of verification code: The length of SMS OTPs sent to users. The valid range of values is 1-6 bit.

Validity period of SMS verification code: The validity period of SMS OTPs. The valid range of values is 1-300 seconds.

← **Create authentication source**

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

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

**Configure SMS policy**

Length of verification code \*  bit

Validity period of SMS verification code \*  seconds



# Email OTP

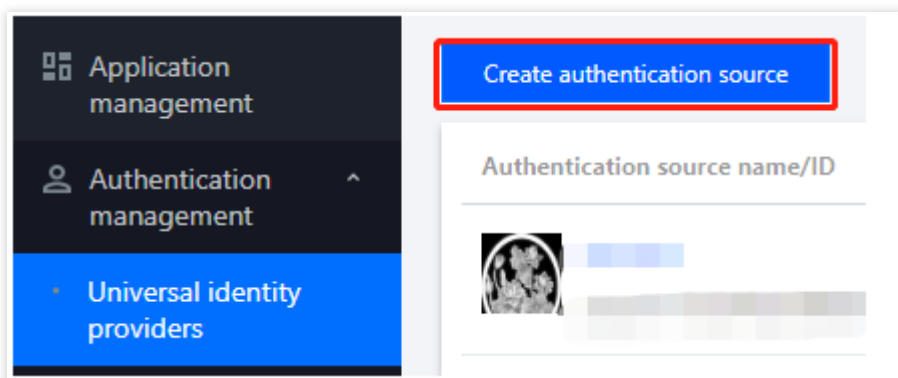
Last updated : 2023-12-22 11:42:07

## Scenarios

Customer Identity and Access Management (CIAM) supports the email OTP authentication source. That is, the system authenticates a user by sending an OTP to the email address of the user.

## Steps

1. Log in to the [CIAM console](#) and select **Authentication management** -> **General authentication source** in the left navigation pane.
2. On the **General authentication source** page, click **Create authentication source**.



3. On the **Create authentication source** page, select **Email OTP** and click **Next**.
4. On the **Create authentication source** page, configure the icon, name, attribute, and description of the authentication source, and then click **Next**.

### Note:

Authentication source icon: The icon displayed in lists and portals. Click **Upload again** to change the default icon.

Authentication source name: A name to identify the authentication source.


Authentication source attribute: The email OTP authentication source uses the email attribute by default. This field cannot be modified.

Authentication source description: A brief description of the authentication source.

← **Create authentication source**

1 **Select an authentication method** > 2 **Configure authentication source**

Authentication source icon \* auth\_email.svg



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

Upload a PNG or JPG file within 1 MB.

Authentication source name \*

Authentication source attribute \*

Authentication source description

[Back](#) [Next](#) [Cancel](#)

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

**Note:**

Email verification code length: The length of email OTPs sent to users. The valid range of values is 1-128 bit.

Email verification code validity: The validity period of email OTPs. The valid range of values is 1-300 seconds.

← **Create authentication source**

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

**Configure email OTP policy**

**Email verification code length \***  bit

**Email verification code validity \***  seconds

# Editing an authentication source

## Username-password authentication

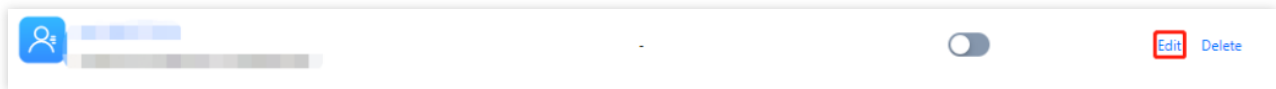
Last updated : 2023-12-22 11:42:07

### Prerequisites

You cannot edit an enabled authentication source. You must disable the authentication source before editing.

### Steps


1. Log in to the [Customer Identity and Access Management console](#) and select **Authentication management** -> **General authentication source** in the left navigation pane.
2. On the **General authentication source** page, select the authentication source to edit and click **Edit**.



3. On the **Basic information** tab, modify the basic information as needed and click **OK** to modify the basic information.

**Basic information** Configure policy

Authentication source icon \* `auth_accountpassword...`



Upload a PNG or JPG file within 1 MB.

Authentication source name \*

Authentication source attribute \*

Authentication source description

4. Click the **Password policies** tab.

5. On the **Password policies** tab, modify the authentication source policy and click **OK** to modify the password policy.

**Note:**

For more information, please see [Policy configuration parameter description](#).

# SMS OTP


Last updated : 2023-12-22 11:42:07

## Prerequisites

You cannot edit an enabled authentication source. You must disable the authentication source before editing.

## Steps


1. Log in to the [Customer Identity and Access Management console](#) and select **Authentication management** -> **General authentication source** in the left navigation pane.
2. On the **General authentication source** page, select the SMS OTP authentication source to edit and click **Edit**.

Authentication source name/ID	Description	On/Off	Operation
 [Redacted]	-	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>

3. On the **Basic information** tab, modify the basic information as needed and click **OK** to modify the basic information.

**Basic information**    Configure policy

Authentication source icon \*    auth\_message.svg

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

Upload a PNG or JPG file within 1 MB.

Authentication source name \*   

Authentication source attribute \*     [✕](#)

Authentication source description   

[OK](#)    [Cancel](#)


4. Click the **SMS policy** tab.

5. On the **SMS policy** tab, modify the authentication source policy and click **OK** to modify the SMS policy.

**Note:**

Length of verification code: The length of SMS OTPs sent to users. The valid range of values is 1-6 bit.

Validity period of SMS verification code: The validity period of SMS OTPs. The valid range of values is 1-300 seconds.

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

**Configure SMS policy**

Length of verification code \*  bit

Validity period of SMS verification code \*  seconds



# Email OTP

Last updated : 2023-12-22 11:42:07

## Prerequisites

You cannot edit an enabled authentication source. You must disable the authentication source before editing.

## Steps

1. Log in to the [Customer Identity and Access Management console](#) and select **Authentication management** -> **General authentication source** in the left navigation pane.
2. On the **General authentication source** page, select the email OTP authentication source to edit and click **Edit**.


Authentication source name/ID	Description	On/Off	Operation
@ [blurred]	-	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>

3. On the **Basic information** tab, modify the basic information as needed and click **OK** to modify the basic information.

**Basic information**    Configure policy

---

Authentication source icon \*                      auth\_email.svg

Upload a PNG or JPG file within 1 MB.

Authentication source name \*                     

Authentication source attribute \*                     

Authentication source description                     

---

4. Click the **Email policy** tab.

5. On the **Email policy** tab, modify the email verification code length and email verification code validity, and then click **OK** to modify the email policy.

**Note:**

Email verification code length: The length of email OTPs sent to users. The valid range of values is 1-128 bit.

Email verification code validity: The validity period of email OTPs. The valid range of values is 1-300 seconds.

Basic information **Configure policy**

**Configure email OTP policy**

**Email verification code length \***    bit

**Email verification code validity \***    seconds

# Testing an authentication source


Last updated : 2023-12-22 11:42:07

## Testing SMS OTPs

1. Log in to the [Customer Identity and Access Management \(CIAM\) console](#) and select **Authentication management** -> **General authentication source** in the left navigation pane.
2. On the **General authentication source** page, select the SMS OTP authentication source to test and click **Test SMS**.

### Note:

The test SMS feature is available only when an SMS OTP authentication source is enabled.

Authentication source name/ID	Description
 [blurred]	-

3. In the **Test SMS** window displayed, enter a mobile number and click **Send test SMS message**. Then, the system sends a test SMS message to the user according to the configuration of the SMS OTP authentication source.

### Test SMS

Mobile number \*

## Testing email OTPs

1. Log in to the [CIAM console](#) and select **Authentication management** -> **General authentication source** in the left navigation pane.
2. On the **General authentication source** page, select the Email OTP authentication source to test and click **Test email**.

### Note:

The test email feature is available only when an email OTP authentication source is enabled.



3. In the Test email window displayed, enter an email address and click Send test email. Then, the system sends a test email to the user according to the configuration of the email OTP authentication source.

**Test email** ×

Mail \*

# Disabling or deleting an authentication source

Last updated : 2023-12-22 11:42:07

## Scenarios

This topic describes how to disable and delete an authentication source in the Customer Identity and Access Management (CIAM) console.

### Note:


Disabling an authentication source will affect the use of the authentication source by applications. Please proceed with caution.

All the data of a deleted authentication source cannot be recovered. Please proceed with caution.

## Disabling an authentication source

1. Log in to the [CIAM console](#) and select **Authentication management** -> **General authentication source** in the left navigation pane.
2. On the **General authentication source** page, select the authentication source to disable and click



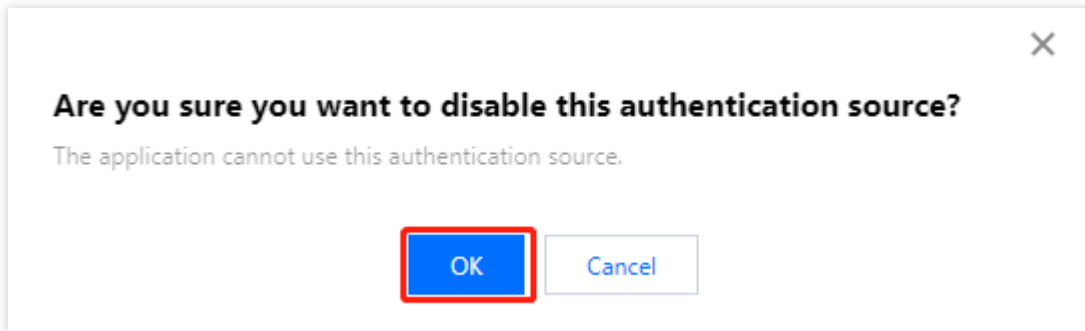
Authentication source name/ID	Description
	-

3. In the confirmation window displayed, click **OK** to disable the authentication source.

### Note:

If the authentication source is configured as the preferred authentication source in the login process of an application, the system will prompt that this source cannot be disabled. If you still need to disable it, unbind this source in the login process first.

If the authentication source is configured as the associated authentication source in the login process of an application, after this source is disabled, the system will prompt that the use of this source by the application will be affected.

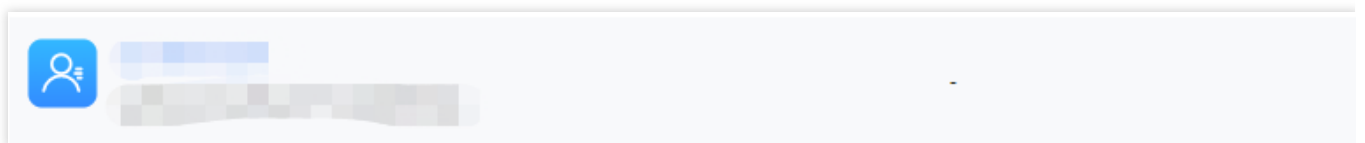


## Deleting an authentication source

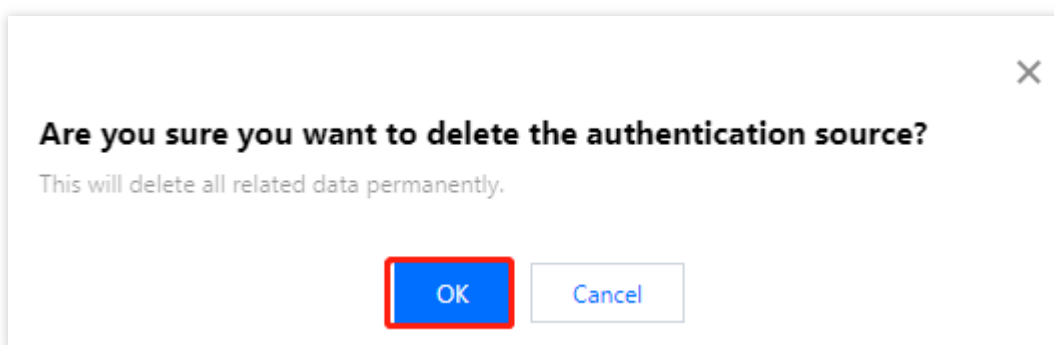
1. Log in to the [CIAM console](#) and select **Authentication management** -> **General authentication source** in the left navigation pane.
2. On the **General authentication source** page, select the authentication source to delete and click **Delete**.

### Note:

If the authentication source is configured as the preferred authentication source in the login process of an application, the system will prompt that this source cannot be deleted. If you still need to delete it, unbind it in the login process first.



3. In the confirmation window displayed, click **OK** to delete the authentication source.



# Audit management

Last updated : 2023-12-22 11:42:08

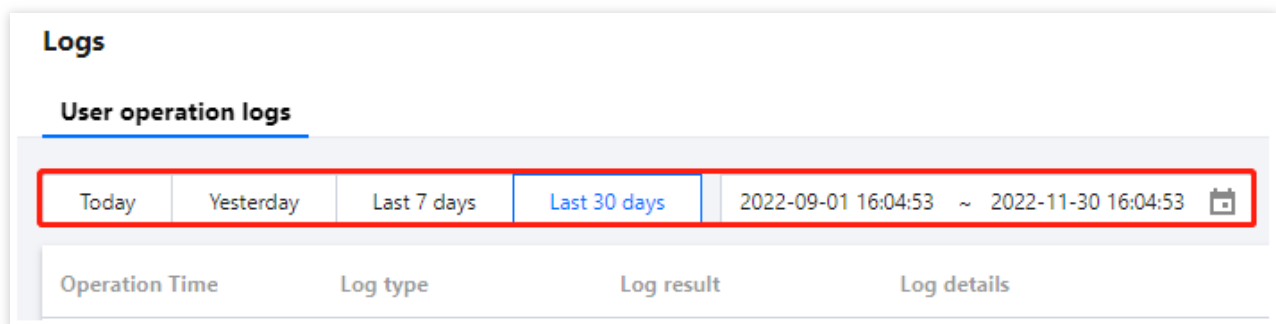
## Scenarios

Audit logs provide a detailed record of the key operations of users on the platform. Administrators can view a record, review an operation, and analyze high-risk actions at any time. This topic describes how to view user operation logs in the Account Risk Control Platform console.

## Steps

1. Log in to the [CIAM console](#) and select **Audit management** -> **User operation logs** in the left navigation pane.
2. On the **User operation logs** page, you can view user operation logs by switching time periods or using the search box.

You can select **Today**, **Yesterday**, **Last 7 days**, or **Last 30 days** to view the logs.



Enter a log type, log result, authentication source, or application in the search box, and then click



to search logs.



**User operation logs**

Today Yesterday Last 7 days **Last 30 days** 2022-09-01 16:04:53 ~ 2022-11-30 16:04:53

Operation Time	Log type	Log result	Log details	Authentication source	Apply	IP address
[REDACTED]	SIGNUP	[REDACTED]	[REDACTED] fully id	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	SIGNUP	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Total items: 2 10 / page 1 / 1 page

# Custom settings

## Domain settings

Last updated : 2023-12-22 11:42:07

### Scenarios

This topic describes how to configure a Tencent Cloud-hosted domain name in the Customer Identity and Access Management (CIAM) console.

**Note:**

If a custom domain name is not configured, the default domain name is used.

### Configuring a Tencent Cloud-hosted domain name

1. Log in to the [CIAM console](#) and select **Custom settings** -> **Domain settings** in the left navigation pane.
2. On the **Domain settings** page, select **Tencent Cloud-hosted domain name**. When a directory is created, the system specifies a Tencent Cloud-hosted domain name as the default domain name, which users can modify. Then, enter the desired domain name and click **Save** to modify the domain name.

**Custom domain name**

Tencent Cloud-hosted domain name  Own domain name

https:// [blurred] .sg.tencentciam.com [Verify domain name](#) ⓘ

**Save**

### Configuring your own domain name

1. Log in to the [CIAM console](#) and select **Custom settings** -> **Domain settings** in the left navigation pane.

2. On the **Domain settings** page, select **Own domain name**. Then, enter your existing domain name and click **Save** to configure the custom domain name.

**Custom domain name**

Tencent Cloud-hosted domain name  Own domain name

https://   ⓘ

# Template settings

## SMS templates

Last updated : 2023-12-22 11:42:07

### Scenarios

By default, Customer Identity and Access Management (CIAM) provides each tenant with a free SMS quota of 50 SMS messages. After a tenant exceeds the free quota, the platform will stop sending SMS messages for the tenant, including console test SMS messages and the OTP SMS messages of authentication sources for portal login. To ensure the normal use of services, administrators need to configure SMS templates to provide SMS services for platform services.

### Configuring SMS templates

1. Log in to the [CIAM console](#) and select **Custom settings** -> **Template settings** -> **SMS message template** in the left navigation pane.
2. On the **SMS message template** tab, click **Edit** in the upper right corner.
3. On the edit page, configure the parameters for SMS service configuration and verification code SMS, and then click **OK**.

### Template settings

**SMS message template**    Email template

---

#### SMS service configuration

\* SMS Service

\* SDK AppID

\* Secret ID

\* Secret Key

#### Verification code SMS

\* Registration verification ⓘ

\* Login ⓘ

\* Two-step authentication ⓘ

\* Modifying mobile number ⓘ

#### SMS service test

**Note:**

Different SMS service configurations require different parameters. The platform currently **only supports Tencent Cloud SMS** and will allow users to configure other SMS services in the future. The following parameters are required to configure Tencent Cloud SMS.

## Configuring Tencent Cloud SMS

### Getting the SDK AppID

1. Log in to the [SMS console](#) and select **Application Management** -> **Application List** in the left navigation pane.
2. On the **Application List** page, click **Create Application**, configure the application name, application intro, and tags, and then click **Create**.

### Create Application

Application Name\*

Application Intro   
0 / 300  
Up to 300 characters

Tag (optional) ⓘ [+ Add](#)

[Create](#) [Cancel](#)

3. On the **Application List** page, select the desired application and click



to copy the SDK AppID of the application.

**Default APP**

SDKAppID:   
Tag: N/A

[Disable](#)

### Getting the SecretId and SecretKey

1. Log in to the [Cloud Access Management console](#) and select **Users** -> **User List** in the left navigation pane.
2. On the **User List** page, select the desired sub-account and click the **username** to go to the **User Details** page.
3. On the **User Details** page, click **API Key**, select the desired key, and then click



to copy the SecretId of the sub-account. Click **Show** and verify your identity to view the SecretKey of the sub-account.

## Configuring SMS templates

To configure SMS templates, you need to obtain the SMS signature and template ID required to send an SMS message in the following ways:

### Getting the SMS signature

1. Log in to the [SMS console](#) and select **Global SMS** -> **Signatures** in the left navigation pane.
2. On the **Signatures** page, click **Create Signature**, fill in the parameters, and then click **OK**.

**Create Signature** Singapore Your data will be stored in Singapore

Signature Purpose  For verified entities (such as websites, applications, official accounts, or mini programs with signatures verified by t)  For unverified entities (such as organizations, websites, or product names with signatures that are not verified by t)

Signature Type\* Select signature type

Signature Content\* Enter signature content  
2-12 characters, supporting Chinese, letters, and numbers. Cannot contain the 【】 symbol. Sample: Tencent Cloud.

Remarks Enter purpose of applying for signature (optional)  
0 / 250  
Enter purpose of applying for signature (optional)

**OK** Cancel

3. Upon approval, you can view the SMS signature on the **Signatures** page.

### Getting the template ID

1. Log in to the [SMS console](#) and select **Global SMS** -> **Body Templates** in the left navigation pane.
2. On the **Body Templates** page, click **Create Body Template**, fill in the parameters, and then click **OK**.

**Create Body Template** Singapore Your data will be stored in Singapore User Feedback Documentation

Template Name\*

SMS Type  Regular SMS  Marketing SMS (available after upgrading to organization verification)

SMS Content\* [Use a Standard Template](#) You can customize your template content or use a standard template. The use of a standard template will improve the review efficiency and approval rate.

Sample template: your login verification code is {1}, which will expire in {2} minutes. If the login was not made by you, ignore this message. {{number}} is customizable and must be consecutively numbered from 1, such as {1}, {2}, and so on

0 / 490

The current template is estimated to be sent in 0 messages.  
(Note: Signature and template variables will affect the number of messages billed)

1. For messages including only English characters, if an SMS message contains 160 characters or less, it will be billed as one message; otherwise, it will be billed as multiple messages based on the standard of 153 characters per message. For example, if an SMS message contains 320 characters, it will be billed as 3 messages (153 + 153 + 14 characters).
2. For messages including non-English characters, if an SMS message contains 70 characters or less, it will be billed as one message; otherwise, it will be billed as multiple messages based on the standard of 67 characters per message. For example, if an SMS message contains 150 characters, it will be billed as 3 messages (67 + 67 + 16 characters).
3. SMS template cannot contain the [ ] symbol
4. It is forbidden to send any finance-related verification codes, system notifications, or marketing SMS messages, as well as illegal SMS messages related to real estate, migration, politics, pornography, and violence. [Details >](#)
5. You are not allowed to set a URL (including short URL) as variable, such as www.{1}.com. [Details >](#)

Temple Sample: {1} is your login verification code, which will expire in {2} minutes. If you did not request for it, ignore this message.{{1} and {2} are customizable and must be consecutively numbered starting from 1, such as {1}, {2}, etc.)

Remarks

0 / 250

- The review will be completed within 2 hours after an SMS template is submitted.
- Review working hours: Monday to Sunday 9:00-23:00 (regardless of public holidays or not)

3. Upon approval, you can view the template ID on the **Body Templates** page.



# Email templates

Last updated : 2023-12-22 11:42:07

## Scenarios

By default, Customer Identity and Access Management (CIAM) provides each tenant with a free email quota of 50 emails. After a tenant exceeds the free quota, the platform will stop sending emails for the tenant, including console test email OTPs and the OTP emails of authentication sources for portal login. To ensure the normal use of services, administrators need to configure email templates to provide email services for platform services.

## Configuring email templates

1. Log in to the [CIAM console](#) and select **Custom settings** -> **Template settings** -> **Email template** in the left navigation pane.
2. On the **Email template** tab, click **Edit** in the upper right corner.
3. On the edit page, configure the parameters for email service configuration and email template settings, and then click **OK**.

### Email service configuration

Email service:

Secret ID:

Secret Key ⓘ:

Sender address:

### Email template settings

Verification code:   
In the email template, the message body must contain otp and time placeholders, and no other placeholders all  
Sample: [Tencent Security] Your email OTP is: {{ otp }} and valid for {{ time }} seconds. Please enter it in time.

Reset password:   
In the password retrieving email template, the message body must contain three placeholders, namely name, ma  
Sample: [Tencent Security]] Dear {{ name }} user, please use the security code {{ mailverifycode }} to reset your pa

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

### Email service test

**Note:**

Different email service configurations require different parameters. The platform currently **only supports Tencent Cloud SES** and will allow users to configure other email services in the future. The following parameters are required to configure Tencent Cloud SES.

## Configuring Tencent Cloud SES

The email template settings support different email gateways. After you select a supported email service, the page dynamically loads the configuration information required by the email service.

## Getting the SecretId and SecretKey

1. Log in to the [Cloud Access Management console](#) and select **Users** -> **User List** in the left navigation pane.
2. On the **User List** page, select the desired sub-account and click the **username** to go to the **User Details** page.
3. On the **User Details** page, click **API Key**, select the desired key, and then click



to copy the SecretId of the sub-account. Click **Show** and verify your identity to view the SecretKey of the sub-account.

### Getting the sender address

1. Log in to the [SES console](#). In the left navigation pane, click **Configuration** -> **Sender Domain**.
2. On the **Sender Domain** page, click **Create**, enter a domain name, and then click **Submit**. The domain name will be used to create the sender address. For more information, please see [Sender Domain](#).

**Create Sender Domain** ✕

Domain

To avoid conflicts between SPF and MX records, do not use corporate email domains. If there is a corporate email domain, create a second-level domain under it and use the second-level domain here.

**Submit** Cancel

3. On the [Sender Address](#) page, click **Create**, configure the parameters, and then click **Submit** to create the sender address. The address will be used to send emails from CIAM.

### Create Sender Address ✕

Sender Domain

Each domain supports up to 10 sender addresses.

Email Prefix  @

Sender Name

Sender Address Preview

## Configuring email templates

1. On the [Email Template](#) page, click **Create**, configure the parameters, and then click **Submit**. Then, you can use the template to call SES.

### Create Email Template ✕

Template Name \*

Template type \* HTML rich text Plain text

Email Summary

Email Body \* 

Choose a file/drag & drop here

Upload an HTML file. Only UTF-8 encoded files are supported. The file size cannot exceed 400KB.

A variable in the email body is expressed with `{{variable name}}`, such as "Dear `{{name}}`". A variable name can only contain letters (a-z, A-Z), digits (0-9), and underscores (`_`).

Submit
Preview
Cancel

**Parameter description:**

Parameter	Description	Parameter template
Template name	A custom name.	-
Template type	Choose one as needed. HTML rich text: Supports more styles to show rich content. Plain text: Supports text only.	-
Template summary	A custom summary.	-
Email body	Verification code: When you apply for a verification code email template, the	Tencent Security: Your email OTP is <code>{{ otp }}</code> . The OTP is valid for <code>{{ time }}</code> seconds.

	email body must contain only the OTP and time placeholders.	
	Reset password: When you apply for a reset password email template, the email body must contain only the name, mailverifycode, and time placeholders.	Tencent Security: Dear {{ name }}, you have requested to reset your password. The verification code for resetting your password is {{ mailverifycode }}. The code is valid for {{ time }} seconds.
	Retrieve username: When you apply for a retrieve username email template, the email body must contain only the name placeholder.	Tencent Security: Dear user, you have requested to retrieve your username {{ name }}.

2. On the **Email Template** page, you can view the template you just created and copy the template ID.
3. In the Email template settings section of CIAM, you need to fill in the IDs of the three approved sending templates: verification code, reset password, and retrieve username.

**Email template settings**

Verification code [ID]

In the email template, the message body must contain otp and time placeholders, and no other placeholders allowed. Sample: [Tencent Security] Your email OTP is: {{ otp }} and valid for {{ time }} seconds. Please enter it in time.

Reset password [ID]

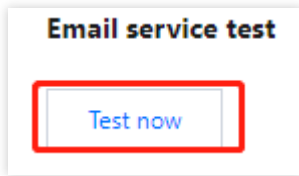
In the password retrieving email template, the message body must contain three placeholders, namely name, mailverifycode, and time. Sample: [Tencent Security] Dear {{ name }} user, please use the security code {{ mailverifycode }} to reset your password.

Retrieve username [ID]

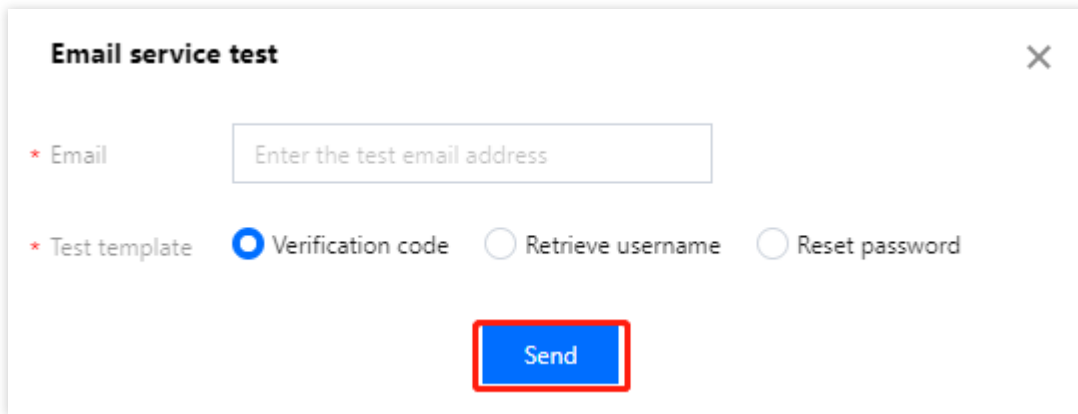
In the username retrieving email template, name is the one and only placeholder in the message body. Sample: [Tencent Security] Dear user, you have retrieved your account: {{ name }}.

## Testing email services

1. After configuring the email template settings, you can click **Test now**.



2. In the **Email service test** window displayed, enter a valid test email address, select a test template, and then click **Send** to verify the configuration.

A screenshot of a web application window titled "Email service test" with a close button (X) in the top right corner. The window contains two required fields: "Email" and "Test template". The "Email" field is a text input box with the placeholder text "Enter the test email address". The "Test template" field has three radio button options: "Verification code" (which is selected), "Retrieve username", and "Reset password". A blue "Send" button is located at the bottom center of the form, highlighted with a red rectangular box.