

OneAccess

User Guide

Issue 01
Date 2024-12-26



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

1 Before You Start	1
2 Buying an Instance	2
3 Instance Management	4
4 Enterprise Administrator Guide	7
4.1 Logging In to the OneAccess Administrator Portal	7
4.2 User Management	8
4.2.1 Managing Users	8
4.2.2 Managing Organizations	17
4.2.3 Managing User Groups	22
4.2.4 Managing Dynamic User Groups	24
4.2.5 Managing Identity Source	26
4.2.6 Managing User Attributes	36
4.2.7 Managing Authorization	41
4.3 Resources	45
4.3.1 Overview	45
4.3.2 Applications	46
4.3.2.1 Adding an Application	46
4.3.2.2 Enabling, Disabling, or Deleting an Application	51
4.3.2.3 General Information	52
4.3.2.4 Authentication Integration	53
4.3.2.5 Synchronization Integration	55
4.3.2.6 Login Configuration	56
4.3.2.7 Access Control	57
4.3.2.8 Object Models	60
4.3.2.9 Authorization Management	64
4.3.2.9.1 Managing Application Accounts	65
4.3.2.9.2 Managing Application Organizations	71
4.3.2.9.3 Managing Synchronization Events	74
4.3.2.9.4 Managing Orphan Accounts	75
4.3.2.9.5 Managing Shared Accounts	77
4.3.2.10 API Permission Management	80
4.3.2.11 Application Permission Management	80

4.3.2.12 Security Settings.....	85
4.3.2.13 Audit Logs.....	85
4.3.3 APIs.....	86
4.3.3.1 Authorizing Access to Built-in APIs.....	86
4.3.3.2 Calling Built-in APIs.....	91
4.3.3.3 Modifying Built-in APIs.....	91
4.3.3.4 Adding a Custom API.....	92
4.3.3.5 Configuring a Custom API.....	92
4.3.3.6 Deleting a Custom API.....	93
4.4 Authentication.....	93
4.4.1 Managing Authentication Providers.....	93
4.4.2 Managing Regions.....	95
4.4.3 Managing Authentication Strategies.....	96
4.5 Security.....	98
4.5.1 Managing Administrator Permissions.....	98
4.5.2 Managing Password Policies.....	103
4.5.3 Managing Risky Behaviors.....	105
4.6 Audit.....	108
4.7 Settings.....	110
4.7.1 Modifying Enterprise Information.....	110
4.7.2 Enterprise Settings.....	111
4.7.2.1 Overview.....	111
4.7.2.2 General Settings.....	111
4.7.2.3 User Agreement Configuration.....	112
4.7.2.4 SMS Gateway.....	114
4.7.2.5 Voice Gateway.....	115
4.7.2.6 Email Gateway.....	117
4.7.2.7 DingTalk Gateway.....	118
4.7.3 Dictionaries.....	120
4.7.4 Data Import and Export.....	122
4.7.4.1 Importing Data.....	122
4.7.4.2 Exporting Data.....	124
4.7.5 UI Settings.....	125
4.7.6 Service Settings.....	135
4.7.7 CloudBridge Agent Configuration.....	139
5 Common User Guide.....	155
5.1 Registering an Account.....	155
5.2 Resetting a Password.....	157
5.3 Logging In to the User Portal and Accessing Applications.....	159
5.3.1 SMS.....	159
5.3.2 OTP.....	161
5.3.3 Password.....	163

5.3.4 Authentication Provider.....	165
5.4 Account Delegation.....	166
5.5 Account Settings.....	166
6 Key Operations Recorded by CTS.....	169
6.1 OneAccess Operations Recorded by CTS.....	169
6.2 Viewing CTS Traces in the Trace List.....	170

1 Before You Start

OneAccess is intended for enterprise administrators and common users.

- Enterprise administrators: the account administrator and users who have administrator permissions for OneAccess. Enterprise administrators manage users, user groups, organizations, applications, and APIs. To learn how to use OneAccess as an enterprise administrator, see [Enterprise Administrator Guide](#).
- Users: enterprise employees, partners, and customers who use enterprise applications. Users log in to OneAccess to access different applications. To learn how to use OneAccess as a user, see [Common User Guide](#).

 **NOTE**

Currently, OneAccess is available in the CN East-Shanghai1 region. To gain access, apply to be added to the whitelist.

2 Buying an Instance

Before using OneAccess, you need to purchase instances as prompted.

- [Register an account and authenticate it.](#)
- [Top up your account.](#)
- [Buy an instance.](#)

Registering an Account and Completing Real-Name Authentication

If you already have an account, buy an instance by referring to [Buying an Instance](#). If you do not have an account, register one by performing the following steps:

- Step 1** Visit the [Huawei Cloud official website](#) and click **Sign Up**.
- Step 2** Sign up for a HUAWEI ID. For details, see [Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services](#).

After the registration is complete, the account information page is displayed.

- Step 3** Perform real-name authentication by following the instructions in [Individual Real-Name Authentication](#) or [Enterprise Real-Name Authentication](#).

----End

Topping Up Your Account

To buy OneAccess instances, ensure that your account has sufficient balance. If your account balance is sufficient, skip this part.

- For details about the pricing of OneAccess, see "OneAccess Pricing Details".
- For details about how to top up your account, see [Topping Up an Account](#)

Buying an Instance

NOTE

Huawei Cloud accounts, authorized member accounts, and delegated accounts can buy OneAccess instances.

After you buy a OneAccess instance, you can use it.

Step 1 Go to the page for buying OneAccess.

Step 2 Configure the parameters on the page for buying OneAccess.

1. Select a region from the **Region** drop-down list.
2. Select an instance specification. Currently, the basic, professional, and enterprise editions are supported.
3. Set user numbers for **Users**.

 **NOTE**

- If you choose the basic edition, the number of users can be 100 or 500.
 - If you choose the professional edition, you can drag the scroll bar to set the number of users. The number of users can be set to 200 or a value ranging from 1000 to 10,000. The number of users between 1000 and 10,000 increases by 1000. To purchase a professional edition instance with more than 10,000 users, [submit a service ticket](#).
 - If you choose the enterprise edition, the number of users is fixed at 40,000 and cannot be changed.
4. Set **Required Duration**. **Auto-renew** is selected by default.
 5. Set **Number of Instances** to an integer ranging from 1 to 100.

 **NOTE**

If you choose the enterprise edition, the number of instances is 1 by default and cannot be changed.

Step 3 Enter and confirm the new administrator password. The default account is the account name of the tenant. The password must contain 8 to 18 characters, including at least three types of the following characters: digits, uppercase letters, lowercase letters, and special characters -+~!@#\$\$%^&*;,;<=>_?`./.

 **NOTE**

Perform this step when the instance specification is an enterprise edition.

Step 4 Click **Next: Confirm**.

Step 5 Select **I have read and accepted <OneAccess Service Statement>** and click **Pay**.

 **NOTE**

- If you select the basic or professional edition, the OneAccess instance will start to be created after you purchase it. After the instance is created, a domain name will be automatically generated.
- If you choose the enterprise edition, submit a [service ticket](#) to enable the instance.

----End

3 Instance Management

This section introduces how to use a OneAccess instance purchased using a Huawei Cloud account. Huawei Cloud accounts can use OneAccess. Member accounts or delegated accounts can use OneAccess only after authorization.

Creating an Authorization

You can authorize specific IAM users to access the administrator portal of the OneAccess instance.

NOTE

You can authorize a maximum of 50 IAM users to access OneAccess.

1. Log in to the Huawei Cloud console.
2. Choose **Service List > Management & Governance > OneAccess**.
3. Click a OneAccess instance.
4. Click **Manage Authorization**. The **Manage Authorization** page is displayed.
5. Click **Add User**. In the displayed dialog box, select an IAM user.
6. Click **OK** to complete the authorization.

NOTE

- By default, IAM users do not have permissions for the **Administrator Permissions** page. For details about other operations, see [Enterprise Administrator Guide](#).
- To grant the IAM user all permissions for OneAccess, select the **OneAccess FullAccess** policy.

Removing an IAM User

To revoke an IAM user's permission to access an instance, perform the following operations:

1. Log in to the Huawei Cloud console.
2. Choose **Service List > Management & Governance > OneAccess**.
3. Click a OneAccess instance.
4. Click **Manage Authorization**. The **Manage Authorization** page is displayed.

5. Click **Remove** in the **Operation** column of the target IAM user.
6. In the displayed dialog box, click **OK**. The IAM user no longer has the permission to access the instance administrator portal.

Customizing Domain Name

You can customize domain names based on your preferences.

1. Log in to the Huawei Cloud console.
2. Choose **Service List > Management & Governance > OneAccess**.
3. Click a OneAccess instance.
4. Click **Customize Domain Name**. The custom domain name page is displayed.
5. Enter a custom domain name in the **Domain Name** text box. The custom domain name must be a subdomain name.
6. Click **Verify Domain Name**. On the **Verify Domain Name** page, click **Verify** to verify the TXT record.
7. After the verification is complete, click **Upload Certificate** to upload the certificate information.
8. Click **Finish**. The custom domain name is configured.

Changing Specifications

On the OneAccess console, you can change the specifications of an instance from the basic edition to the professional edition or change the number of users of the instance. However, the number of users can only be increased but cannot be decreased.

NOTE

You cannot change the specifications of the enterprise edition or change the basic or professional edition to the enterprise edition.

1. Log in to the Huawei Cloud console.
2. Choose **Service List > Management & Governance > OneAccess**.
3. Locate the target OneAccess instance and click **Modify** in the **Operation** column. You can also click the target OneAccess instance to go to the instance details page and click **Modify** in the **Edition** Area.
4. Specify the required instance specifications.

NOTE

- Changing specifications can only increase the number of users, and the professional edition cannot be changed to the basic edition.
 - If the original specification is the basic edition and the number of users is 100, you can change it to the basic edition with 500 users or to the professional edition with configurable number of users.
 - If the original instance is of the basic edition and the number of users is 500, the instance can only be changed to the professional edition and the number of users ranges from 1000 to 10,000.
5. Click **Confirm** to confirm the new specifications.
 6. Click **Submit**.

Renewing and Unsubscribing from Instances

- OneAccess instance can be billed only in the yearly/monthly mode. When it expires, you can click **Renew** on the Huawei Cloud OneAccess console or go to the [Renewal Management](#) page to renew the instance. For details, see [Renewal Management](#).
- To stop using yearly/monthly resources, click **Unsubscribe** on the OneAccess console. The renewed part and currently used part are included. You cannot use these resources after unsubscription. A handling fee will be charged for unsubscribing from an instance. You can click **Unsubscribe** on the Huawei Cloud OneAccess console to unsubscribe from the instance.

4 Enterprise Administrator Guide

4.1 Logging In to the OneAccess Administrator Portal

After subscribing to OneAccess, log in to the administrator portal.

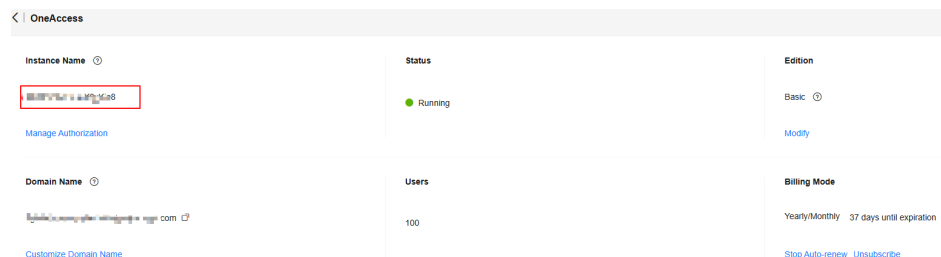
Prerequisites

- You have registered a Huawei ID and completed real-name authentication.
- You have purchased an instance by referring to [Buying an Instance](#).

Procedure

You can access the OneAccess administrator portal in either of the following ways:

- Perform the following steps to access the administrator portal of a OneAccess instance through the console:
 - a. Log in to the Huawei Cloud console.
 - b. Choose **Service List > Management & Governance > OneAccess**.
 - c. On the instance list page, click the target OneAccess instance.
 - d. Click the name of the instance to be accessed to go to the OneAccess instance administrator portal.

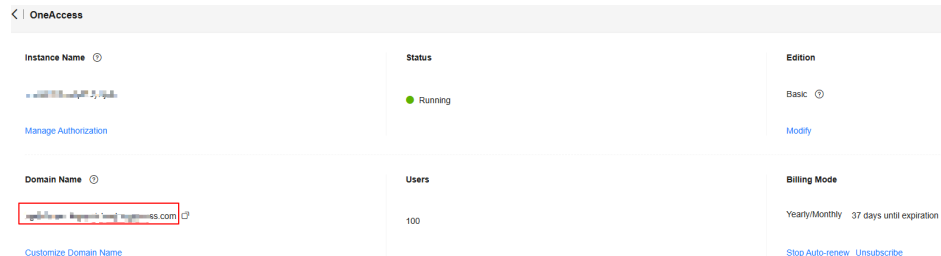


Instance Name	Status	Edition
OneAccess	Running	Basic
Domain Name	Users	Billing Mode
example.com	100	Yearly/Monthly 37 days until expiration

If you do not have the permission to access the OneAccess instance, you need to access the OneAccess administrator portal as an IAM user. For details, see [Granting IAM Users the Permission to Access OneAccess Instance](#).

- Log in to the OneAccess administrator portal using the domain name.

- a. Log in to the Huawei Cloud console.
- b. Choose **Service List > Management & Governance > OneAccess**.
- c. Click the OneAccess instance to be accessed.
- d. Obtain the administrator access domain name.

Figure 4-1 Obtaining the administrator access domain name**NOTE**

The administrator access domain name is generated when you buy a OneAccess instance.

- e. Add an administrator by referring to **Managing Administrator Permissions**.
- f. Use *administrator access domain name/admin*, for example, **https://example.com/admin** to access the OneAccess administrator portal.
- g. Enter the administrator username and password, and click **Log in**.

4.2 User Management

4.2.1 Managing Users

Create, modify, and delete users in the administrator portal.

To add a large number of users, synchronize user data from your identity sources or import user data with a template.

- Import from identity sources: Configure data import logic to synchronize identity data from upstream identity sources to OneAccess. For details, see **Identity Sources**.
- Import with a template: Add user data to the template and then import the user data to OneAccess. For details, see **Importing Users**.


Creating a User

On the OneAccess administrator portal, you can create an organization for one user or create a user that belongs to multiple organizations.

If the created user belongs to multiple organizations, for example, organization A has the permission to access application C, organization B to application D, and the user has the permissions of both organizations A and B, the user can access applications C and D at the same time after logging in to the user center.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Users > Organizations and Users**.
- Step 3** On the **Organizations and Users** page, click the **Users** tab.
- Step 4** Click **Create User** and set basic user information by referring to [Table 4-1](#).

Table 4-1 Basic information

Attribute	Description
Username	<p>You can determine whether this is mandatory by referring to Modifying User Attributes. If no username is specified, the system automatically generates a username. You can set the character and length by referring to Modifying User Attributes. The username of the new user cannot be the same as those of other users. The username is case insensitive.</p>
Organization	<p>You can specify an organization to which the user to be added belongs. You can select one or more organizations. By default, the first selected organization is the main organization. For details about how to add an organization, see Adding an Organization.</p> <p>NOTE</p> <ul style="list-style-type: none"> • If you select an organization in the organization tree on the left and then click Create User, the selected organization is the main organization by default. • A user can have up to one primary and nine secondary organizations. You can click  on the right of the username and select Change Organization. In the displayed dialog box, adjust the organization.
Name	<p>You can set whether this is mandatory and the length of the character string by referring to Modifying User Attributes.</p>
Cell phone number	<p>You can set whether this is mandatory and the length of the character string by referring to Modifying User Attributes. This must be unique.</p>

Attribute	Description
Email	You can set whether this is mandatory by referring to Modifying User Attributes and the length of the character string. This must be unique.
Area	Select the user's country or region. You can set whether this is mandatory by referring to Modifying User Attributes .
City	Enter the city where the user is located. You can set whether this is mandatory and the length of the character string by referring to Modifying User Attributes .

 NOTE

- The user can log in to the user portal using their username, mobile number, or email address.
- If you manage the user's password, a password link will be sent to the email address or mobile number of the user.
- If the user forgets the password, the user can reset it using the bound email address or mobile number.
- Set a password for the user so that the user can log in to the user portal if no other login authentication mode is enabled.

Step 5 To enable password login, click  . Two ways are provided for login passwords for users:

- Custom: You can customize the user login password.
 - If **Reset password at first login** is selected, users need to change the login password when logging in to the user portal for the first time.
 - If **Reset password at first login** is not selected, users do not need to change the login password when logging in to the user portal for the first time.
- Automatic: A password is automatically generated. The system notifies the user of the initial password and the user must log in to the system within the validity period. If the initial password configuration is not enabled, configure it by referring to [Password Initialization Settings](#).

Step 6 If you want to add the work information of a user, click **Enter more information** on the **Create User** page and enter the work information by referring to [Table 4-2](#).

Table 4-2 Work information

Information	Description
Employee ID	Enter an employee ID. You can set whether the attribute is mandatory and the length of it by referring to Modifying User Attributes .
Manager ID	Enter the immediate supervisor of the user. You can determine whether this is mandatory by referring to Modifying User Attributes .
User Type	You can select the type, such as regular, intern, labor dispatch, and labor outsourcing.
Hire Date	Set the enrollment time of a user. Specify whether this is mandatory and the time range by referring to Modifying User Attributes .
Work Place	Set the working location of a user. Specify whether this is mandatory and the character length by referring to Modifying User Attributes .

 **NOTE**

User information includes basic and work attributes. Set attributes on the **User Attributes** page. For details, see [User Attributes](#).

Step 7 Click **OK**.

----End

Viewing User Details

In the user list, click a user to view its basic information, user groups, applications, and audit logs.


- Basic information
Basic and extended attributes of the user.
- User groups
 - Information about the user groups to which the user belongs, including user group names, organization paths, and applications that the user has been authorized to access.
 - To add the user to more user groups, click **Select Groups**. For details, see [Adding a User to One or More User Groups](#). If user group-based automatic authorization is enabled for an application, the user added to an authorized user group will be synced to the application. For details, see [Configuring Authorization Policies for Application Accounts](#).

- To remove the user from a user group, click **Delete** in the **Operation** column of the row that contains the group.
If user group-based automatic authorization is enabled for an application, the user deleted in an authorized user group will be synced to the application. For details, see [Configuring Authorization Policies for Application Accounts](#).
- Applications
 - Applications that the user has permission to use, including the logo, application name, and application account.
 - To grant the user access to more applications, click **Authorize** in the upper right. For details, see [Granting Application Access to a User](#).
 - If application-side permission is enabled for an application, click **Application Roles/Permissions** in the **Operation** column to grant permissions to the user. The method of granting permissions is similar to that of granting permissions to an application account. For details, see [Application Roles and Permissions](#). For details about how to configure permissions on the application side, see [Application Permission Management](#).
 - To cancel application access of the user, click **Delete** in the **Operation** column of the row that contains the application.
- Audit logs

Audit logs record the operations of enterprise administrators and the user.

 - Administrator logs
Administrators' operations on the user, such as changing the password and authorizing application access. Set filter conditions to view desired logs.
 - User logs
The user's operations (SSO login and logout) in the user portal and access to applications. Set filter conditions to view desired logs.

Modifying User Information

- Step 1** In the user list, move the cursor to the status bar on the right of the username and click . The **Modify User** dialog box is displayed.
- Step 2** Modify the basic information and additional details about a user. For example, whether the user belongs to one or more organizations.

Modify User ×

essential information

Username

* Organization

Name

Cell phone number

Email

area

city

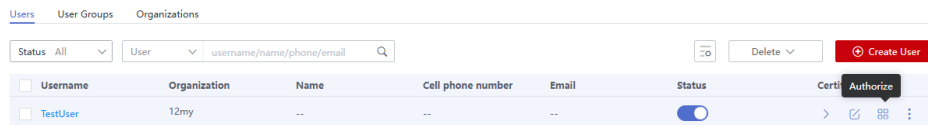
[Enter more information](#)

Step 3 Click **OK**.

----End

Granting Application Access to a User

Step 1 In the user list, move the cursor to the status bar on the right of the username and click . The **Applications** tab page is displayed. For details about how to add an application, see [Integrating Enterprise Applications](#).



Step 2 On the **Applications** tab page of the user details page, click **Authorize**.


Step 3 Select the applications you want to authorize the user to access, and click **Save**. In the list of selected applications, set account names. To set other account attributes, click the application name. By default, the username is used as the application account name. For details about how to grant permissions to users in an application, see [Authorization Management](#).

----End

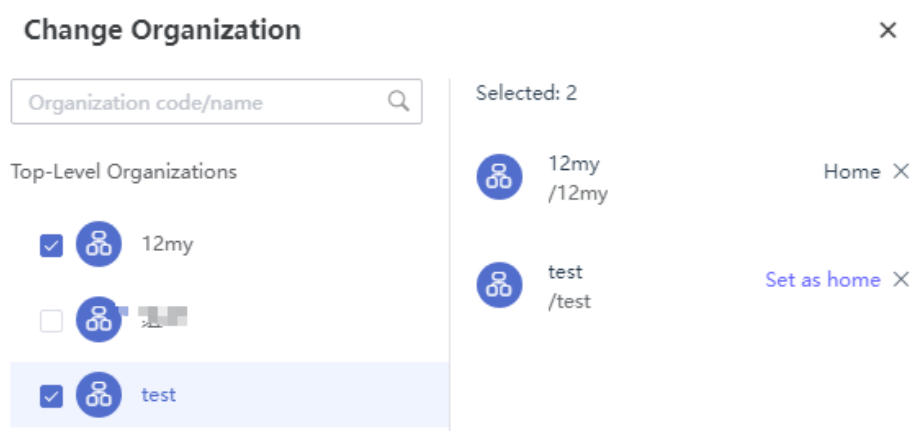
Changing the Organization of a User

By adjusting the organization:

- You can change the organization to which a user belongs.
- You can change a user that belongs to only one organization to multiple organizations.
- You can change a user that belongs to multiple organizations to just one.

Step 1 In the user list, move the cursor to the status bar of the target user, click , and select **Change Organization**.

Step 2 In the displayed dialog box, select a target organization. You can select one or more organizations. By default, the first selected organization is the main organization. If there are multiple organizations, you can click **Set as home** next to the target organization to set it as the main organization.




Step 3 Click **OK**.

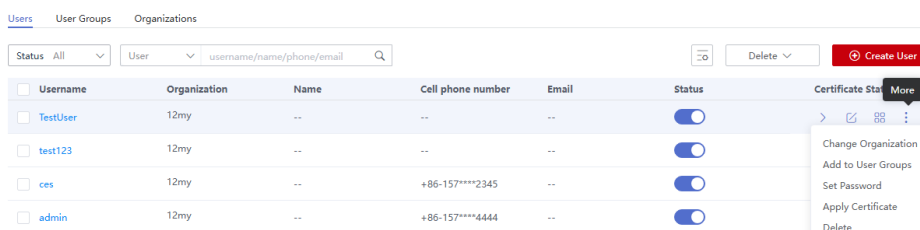
 **NOTE**

If you have enabled **automatic user authorization** for an application, changing the organization of a user will change the user's access to the application. For details, see [Configuring Authorization Policies for Application Accounts](#).

----End

Adding a User to One or More User Groups

Step 1 In the user list, click  in the row that contains the target user and click **Add to User Groups**. The **User Groups** tab page is displayed.




Step 2 On the user details page, click **Select Groups**.

Step 3 Select user groups to which the user will belong, and click **Save**. To remove the user from a user group, click **Delete** in the **Operation** column of the row that contains the group.

----End

Managing User Password

The password can be customized or automatically generated. You can change and reset the user password as needed. For details about how to set the password, see [Managing Password Policies](#).

- Custom
 - a. In the user list, click  in the row that contains the target user and select **Set Password**.
 - b. Select a password generation mode. The default is **Set now**. You can enter a custom password for user login.
 - By default, **Rest password at first login** is selected. When a user uses a new password to log in to the user portal for the first time, the user is required to change the password.
 - If **Rest password at first login** is not selected, the user does not need to change the password for the first login with the new password.

Set Password ✕


* Password Type Set now
Set a password now.

Reset password at first login

Automatically generated
A password will be automatically generated and then sent to the user by email or SMS.

Cancel

Save

- c. Click **Save**. The user password management is complete.
- Automatically generated
 - a. In the user list, click  in the row that contains the target user and select **Set Password**.
 - b. Select **Automatically generated** for **Password Type**.

Set Password ✕

Password Type Set now
 Set a password now.

Automatically generated
 A password will be automatically generated and then sent to the user by email or SMS.

* Notification Method Email SMS

Language Chinese English


- c. Select a notification method and language. Users will receive SMS or email notifications about password resetting based on the notification method you select, and use the new password to log in to the user portal.

NOTE

- After the password is reset, the user is required to change the password when logging in to the user portal for the first time. For details about the password requirements, see [Managing Password Policies](#).
- If you want to notify users by email, configure the email gateway. For details, see [Email Gateway](#).

- d. Click **Save**. The user password management is complete.

Deleting a User

Step 1 In the user list, click  next to a user and click **Delete**.

Step 2 Click **OK**.

NOTE


Deleted users can no longer access the user portal. To add them back, see [Creating a User](#).

----End

Deactivating a User

NOTE

Deactivated users can no longer access the user portal. Exercise caution when performing this operation.


Step 1 In the user list, click  in the **Status** column of the row that contains the target user. By default, new users are active.

Username	Organization	Name	Cell phone number	Email	Status	Certificate State
TestUser	12my	--	--	--	<input checked="" type="checkbox"/>	● Not applied
test123	12my	--	--	--	<input type="checkbox"/>	● Not applied

Step 2 Click **OK**.

----End

Activating a User

Step 1 In the user list, click  in the **Status** column of the target user.

Username	Organization	Name	Cell phone number	Email	Status	Certificate State
TestUser	12my	--	--	--	<input type="checkbox"/>	● Not applied

Step 2 Click **OK**.

----End

4.2.2 Managing Organizations

Organizations facilitate user management and authorization. You can create, modify, move, and delete organizations, and add users to organizations. For details about organization-based authorization, see [Configuring Authorization Policies for Application Organizations](#).

To add a large number of organizations, synchronize organization data from your identity sources or import organization data with a template.

- Import from identity sources: Configure data import logic to synchronize organization data from upstream identity sources to OneAccess. For details, see [Managing Identity Source](#).
- Import with a template: Add organization data to the template and then import the organization data to OneAccess. For details, see [Organizations](#).

Adding an Organization

In an organization tree, you can add top-level organizations and sub-organizations.

Step 1 Log in to the administrator portal.

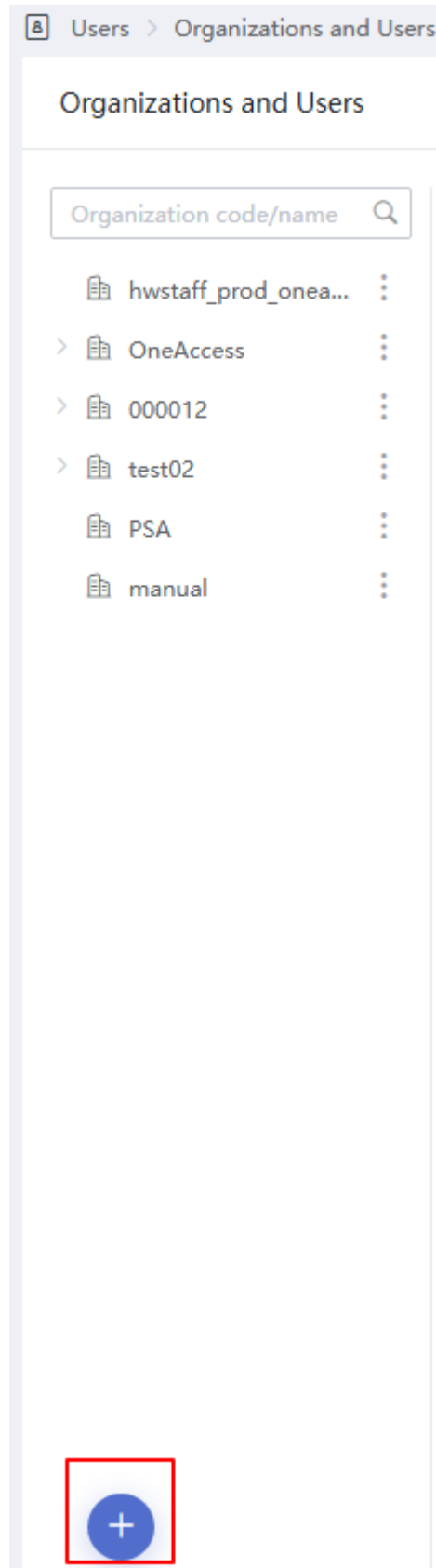
Step 2 On the top navigation bar, choose **Users > Organizations and Users**.


Step 3 On the **Organizations and Users** page, switch to the **Organizations** tab.

Step 4 On the organization list page, click **Create Organization**.

 **NOTE**

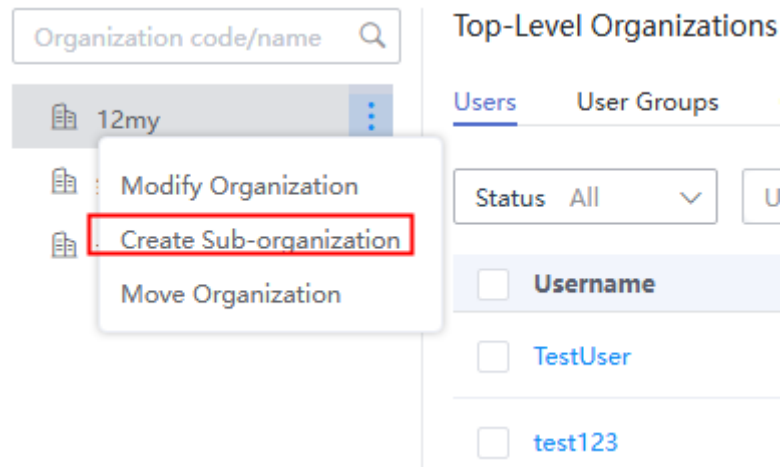
- To create a top-level organization, click the plus sign (+) in the lower left (see the following figure).



- In the organization tree on the left, click  on the right of the organization and select **Create Sub-organization** by referring to [Figure 4-2](#), to quickly add a sub-organization.

Alternatively, select the added top organization in the organization navigation tree on the left and click **Create Organization** to add a sub-organization.

Figure 4-2 Creating a sub-organization



Step 5 On the **Create Organization** page, specify organization parameters.

Table 4-3 Organization information

Parameter	Description
* Organization Type	You can select an organization type from the drop-down list box. The options are Department , Unit , Company , and Group .
* Organization Code	Unique identifier of the organization.
*Organization Name	Organization name. Organizations at the same level must have different names.
Sequence	Position of the organization in the organization tree. By default, new organizations are displayed at the end.
Parent Organization	<ul style="list-style-type: none"> • Leave this parameter empty when adding a top organization. • Displayed as the organization you selected when you create a sub-organization

Step 6 Click **OK**.

----End

Viewing Organization Details

In the organization list, click the target organization and view administrators' operations on it, such as creation and modification. Set filter conditions to view desired logs.

Modifying an Organization

In the organization list, click **Modify** in the row that contains the target organization, and modify the ID, name, and position. You can move an organization to another parent organization. For details, see [Moving an Organization](#).


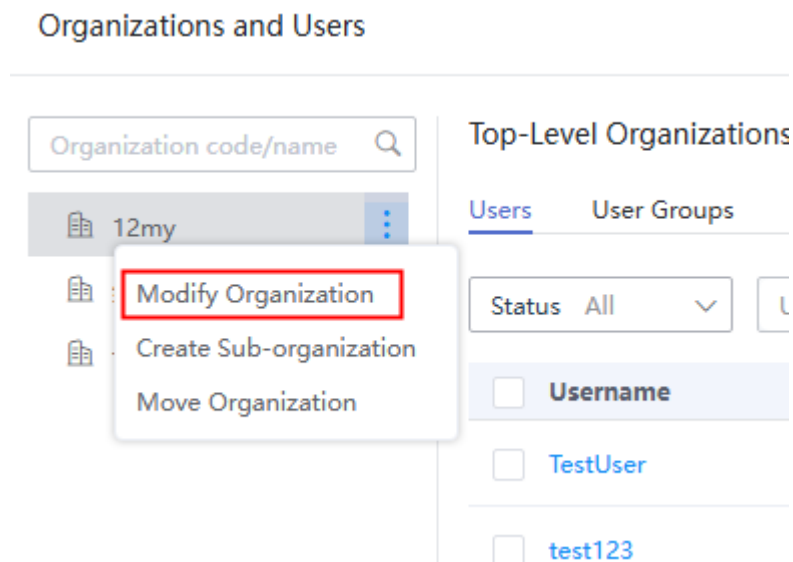

To modify an organization, select it in the left pane, choose  > **Modify Organization** (see [Figure 4-3](#)).

Figure 4-3 Modifying an organization



Moving an Organization

Move an organization to another parent organization. If you have enabled automatic user authorization for an application, moving the organization of a user will change the user's access to the application. For details, see [Configuring Authorization Policies for Application Accounts](#).

Step 1 In the organization list, locate the target organization and click **Move** in the **Operation** column. The **Select Organization** dialog box is displayed. Alternatively, in the organization tree on the left, click  on the right of the organization and click **Move Organization** to quickly move the organization.

Step 2 In the **Select Organization** dialog box, select an upper-level parent organization.

 **NOTE**

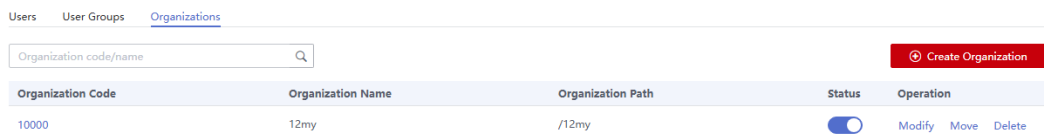
- If the organization to be moved is a sub-organization and you want to set it as the top organization, click **Set as Top-level organizations**.
- If the organization to be moved is not a sub-organization, you only need to select the top-level organization in the **Select Organization** dialog box.

Step 3 Click **OK**. In the displayed dialog box, click **OK**.

----End

Deleting an Organization

Step 1 In the organization list, click **Delete** on the right of the target organization.



Organization Code	Organization Name	Organization Path	Status	Operation
10000	12my	/12my	<input checked="" type="checkbox"/>	Modify Move Delete

Step 2 In the displayed dialog box, click **OK** to delete the organization.

 **NOTE**

- The organization cannot be recovered once deleted. Exercise caution when performing this operation.
- If an organization contains users, user groups, or sub-organizations, the organization cannot be deleted. You need to delete the users, user groups, or sub-organizations before deleting the organization.

----End

4.2.3 Managing User Groups

User groups facilitate user management and authorization. You can create, modify, and delete user groups, and add users to them. For details about user group-based authorization, see [Configuring Authorization Policies for Application Accounts](#).

Adding a User Group

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > Organizations and Users**.

Step 3 On the **Organizations and Users** page, click the **User Groups** tab.

Step 4 Click **Create User Group**.

Step 5 In the **Create User Group** dialog box, select an organization, enter the user group name and description, and select an application scenario.

Step 6 Click **OK**.

----End

Viewing User Group Details

In the user group list, click a user group to view its members, applications, and audit logs. For details about how to view and operate a dynamic user group, see [Managing Dynamic User Groups](#).

- Manage members: You can view information about users in a user group, such as the username, mobile number, and email address.
 - On the **Members** tab page of the user group details page, click **Add Member** in the upper right corner of the user group list and select the users to be added to the user group. For details, see [Adding Users to a User Group](#).

Username	Full Name	Phone Number	Email Address	Organization	Status	Join time
TestUser				f12my	Disabled	2024-11-11 14:03:48
test123				f12my	Normal	2022-09-23 15:03:07

- On the **Members** tab page of the user group details page, click **Delete** in the **Operation** column to delete a user from the user group. For details, see [Deleting a User Group](#).

- Applications that the user group has been authorized to access, including the logo and application name.

If you click **Delete** in the **Operation** column of the row that contains an application, the user group will be automatically deleted from the account authorization policy of the application. Then, member addition and deletion for the user group will be automatically synced to the application.

Application Logo	Application Name	Application Accounts	Shared Account	Status	Operation
	SAML	12my		<input checked="" type="checkbox"/>	Authorize by Role/Permission Delete
	LDAP	12my		<input checked="" type="checkbox"/>	Authorize by Role/Permission Delete

- Audit Logs
Administrators' operations on the user group, such as group creation and member addition. You can filter data by time, administrator username, or name.

Modifying User Group Information

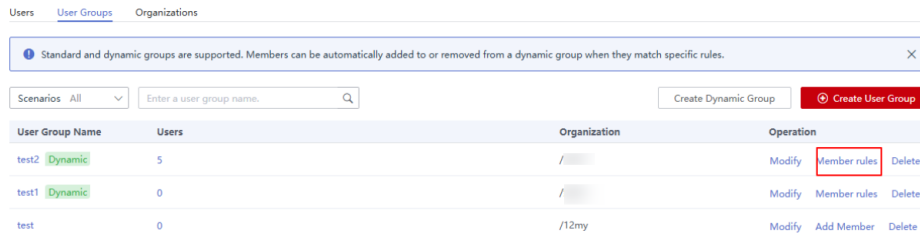
- Step 1** In the user group list, click **Modify** to the right of the user group.
- Step 2** In the **Modify User Group** dialog box, modify the name and description of the user group. The organization to which the user group belongs cannot be changed.
- Step 3** Confirm the configuration.

----End

Adding Users to a User Group

Add members of different organizations to a user group for easy management and authorization. For details about user group-based authorization, see [Configuring Authorization Policies for Application Accounts](#).

Step 1 In the user group list, click **Add Member** in the **Operation** column.

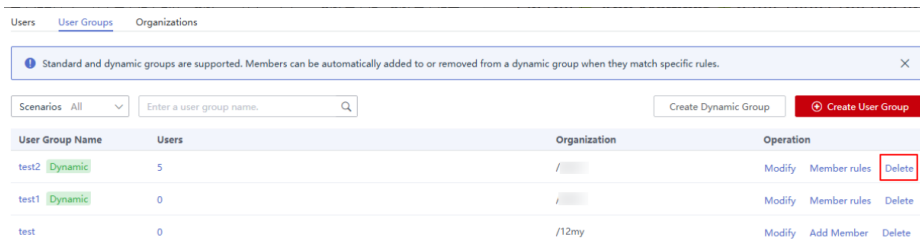


Step 2 On the **Add Member** page, select the top organization, select users under the organization, and click **OK**.

----End

Deleting a User Group

In the user group list, click **Delete** in the row that contains the target user group and click **OK**. Deleting a user group will not delete the users, but will affect their application permissions. For details about user-based authorization, see [Configuring Authorization Policies for Application Accounts](#).



4.2.4 Managing Dynamic User Groups

On the OneAccess administrator portal, you can create dynamic user groups and automatically add users to user groups based on member rules (member matching scope, matching rule, calculation rule, and blacklist and whitelist). In addition, you can add, edit, and delete dynamic user groups as required. For details about dynamic user group-based authorization, see [Configuring Authorization Policies for Application Accounts](#).

Adding a Dynamic User Group

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Users > Organizations and Users**.
- Step 3** On the **Organizations and Users** page, click the **User Groups** tab.
- Step 4** Click **Create Dynamic Group**.
- Step 5** In the **Create Dynamic Group** dialog box, select an organization, enter a user group name and description, and select an application scenario.
- Step 6** Click **Next** and enter a dynamic user group member rule.
 1. Member matching range: Click **Select** to select an organization. You can select **Include sub-organizations**, **Exclude sub-organizations**, or **Include**

sub-organizations but exclude some organizations to limit the member matching scope.

 **NOTE**

- If you select **Exclude sub-organizations**, the system searches for only the members that meet the filtering rules among the immediate members of the selected department.
 - If you select **Include sub-organizations** but exclude some organizations, you need to set the lower-level organizations to be excluded.
2. **Matching rules:** Select an attribute, select restriction conditions, and enter values to restrict the attributes of a user. The restrictions include greater than, less than, equal to, not equal to, and including. You can click **Add Rules** to add multiple matching rules.
 3. **Algorithm rules:** define the relationship between multiple rules added in [Step 6.2](#). The default relationship is **AND**. You can adjust the relationship as required.
 4. Select a user and add it to the blacklist or whitelist.

Step 7 Click **OK**.

----**End**

Viewing Details About a Dynamic User Group

In the user group list, click the name of a dynamic user group to view its details, including the user group information, matched members, authorized applications, and audit logs.

- **Details:** You can view the basic information (name, organization, description, and application scenario) and member rules (member matching range, matching rule, calculation rule, and blacklist and whitelist) of a dynamic user group.
- **Members:** You can view the information about the matched members in the dynamic user group, such as the username, mobile number, and email address.

Click **Member Count** in the upper right corner of the user group member list to automatically add users who meet the member rule to the dynamic user group.

- **Applications** that the user group has been authorized to access, including the logo and application name.

If you click **Delete** in the **Operation** column of the row that contains an application, the user group will be automatically deleted from the account authorization policy of the application. Then, member addition and deletion for the user group will be automatically synced to the application.

- **Audit logs:** You can view the operations performed by the administrator on the user group, such as adding members and calculations. You can filter data by time, administrator username, or name.

Modifying Dynamic User Group Information

Step 1 In the user group list, click **Modify** in the **Operation** column of the dynamic user group to be modified.

Step 2 In the **Modify User Group** dialog box, modify the name, description and application scenario of the user group. The organization to which the user group belongs cannot be changed.

Step 3 Click **OK**. The dynamic user group is modified.

----End

Editing Member Rule

You can modify a member rule to add members of different organizations to the same user group for unified management and authorization. For details about user group-based authorization, see [Configuring Authorization Policies for Application Accounts](#).

Step 1 In the user group list, click **Member rules** in the **Operation** column on the right of the dynamic user group.

Step 2 On the page for modifying a member rule, select the member matching range, enter the matching rule, select the blacklist and whitelist users, and click **Submit Calculation**. The member rule is modified.

----End

Deleting a Dynamic User Group

In the user group list, click **Delete** in the **Operation** column on the right of the dynamic user group and click **OK** to delete the dynamic user group. Deleting a dynamic user group will not delete the users, but will affect their application permissions. For details about user-based authorization, see [Configuring Authorization Policies for Application Accounts](#).

NOTE

A dynamic user group associated with an application cannot be deleted.

4.2.5 Managing Identity Source

OneAccess synchronizes identity data using the "Upstream – Midstream – Downstream" model. Upstream refers to an identity source for enterprise management, midstream is OneAccess, and downstream indicates an application system that synchronizes identity data with the upstream. In this model, OneAccess synchronizes identity data in upstream systems to downstream application systems in real time, ensuring consistency, accuracy, and security of identity data throughout the user lifecycle, covering onboarding, job transfer, and resignation.

An identity source is similar to the identity management system of an enterprise. It stores the details of enterprise users. OneAccess supports standard identity sources, such as WeCom, DingTalk, Active Directory (AD), and Lightweight Directory Access Protocol (LDAP). With only simple configuration, you can synchronize organization and user data of these identity sources to OneAccess. Identity source synchronization suits the following scenarios:

- Single identity source

Enterprises that have a single identity source can maintain identity data using its management system.

- Multiple independent identity sources

Enterprises that have multiple independent identity sources can maintain identity data in each identity source using its management system. For example, a company has subsidiaries A and B, which have separate identity management systems and correspond to different organizations in OneAccess. The two subsidiaries can main identity data using their own identity management system.

- Multiple related identity sources

Enterprises that have multiple related identity sources are advised to create and update identity data through a single source to prevent data overriding during synchronization.

OneAccess allows enterprises to synchronize user and organization information from multiple identity sources. The configuration information varies depending on the identity source. For details, see:

- For details about how to add an AD identity source, see [Integrating AD Identity Sources](#).
- For details about how to add an LDAP identity source, see [Integrating LDAP Identity Sources](#).

This section describes how to add an identity source. AD identity is used for illustration.

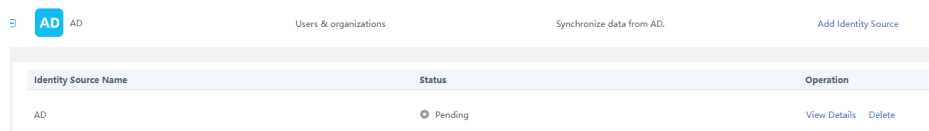
Procedure

Step 1 Add an identity source in OneAccess.

1. Log in to the administrator portal.
2. On the top navigation bar, choose **Users > Identity Sources**.
3. On the **Identity Sources** page, click **Add Identity Source** in the **Operation** column of the row that contains **AD**, enter an identity source name, and click **OK**.

Step 2 Configure the import settings.

1. In the AD identity source list, click **View Details** in the row that contains the target identity source.



2. Click the **Import Settings** tab, set import parameters, and click **OK**.
 - **Basic Settings:** Connection parameters of your AD server to be connected to OneAccess.

Table 4-4 Basic settings

Parameter	Description
* Host	Host name or IP address of the AD server.
*TCP Port	TCP/IP port of the AD server. The default port is 389 . NOTE OneAccess can be accessed only over public networks. Provide the public network address of your server and enable port 389 .
SSL	Default value: true , which indicates that SSL is used to connect the AD server.
StartTLS	Whether to enable startTLS for encrypted communication. <ul style="list-style-type: none"> ▪ true: StartTLS is enabled, and SSL cannot be set to true. ▪ false: Disable StartTLS.
Certificate Verification	Whether to verify the certificate. This parameter is valid only when SSL or StartTLS is set to true . true : Verify the certificate. false : Do not verify the certificate. The certificate must be authenticated by the public network. Self-signed certificates cannot be used.
Protocol Version	Default value: TLSv1.2 . Recommended: TLSv1.3 and TLSv1.2 .
Principal	Identifier used for AD server authentication. Specify an account that has read permission for the AD domain. The input parameter will contain the domain name, for example, admin@test.com and TEST\admin .
*Password	Password of the principal account.
* Base Contexts	One or more root nodes (for example, OU=huaweitest,DC=test,DC=com) in the AD tree to be considered as the beginning for synchronizing AD users.
*UID Attribute	Name of the AD attribute mapped to the UID attribute.
* Account Object Class	One or more object classes to be used when a new user object is created in the AD tree. If you enter multiple object classes, each item occupies a line. Do not use commas (,) or semicolons (;) to separate multiple object classes. Some object classes may require you to specify all object classes in the class hierarchy.

- Optional settings: Whether to synchronize passwords, password attributes to be synchronized, account and organization object classes. Modify these settings if a synchronization error occurs. For certain parameters, you may retain the default settings.

Table 4-5 Optional settings

Parameter	Description
Domain	If a domain name exists, it should be excluded from the reclaimed username. If there are multiple domain names, separate them with commas (.). The default username excludes the domain name.
Account Username Attribute	Saves one or more attributes of an account username. During authentication, these attributes are used to search for the AD entry of the username to be authenticated.
Organization Object Class	One or more object classes that will be used when a new organization object is created in the AD tree. If you enter multiple object classes, each item occupies a line. Do not use commas (,) or semicolons (;) to separate multiple object classes. Some object classes may require you to specify all object classes in the class hierarchy.
Organization Name Attribute	Stores one or more attributes of the organization name. During authentication, these attributes are used to search for the AD entry of the organization name to be authenticated.
Failover Servers	Lists all servers that will be used for failover when the preferred server fails. If the preferred server fails, JNDI will connect to the next available server in the list. Lists all servers in the " ldap:// ldap.example.com:389/ " format (compliant with the standard AD v3 URL described in RFC 2255). Only the host and port parts of the URL are relevant in this setting.

Parameter	Description
Password Attribute	Name of the AD attribute used to store passwords. When the password of a user is changed, a new password will be set for this attribute.
AD Filter	Optional AD filter used to control the accounts returned from AD resources. If no filter is specified, only accounts containing all specified object classes are returned.
Password Hash Algorithm	Algorithm used by the identity system to hash passwords. Currently, SSHA , SHA , SMD5 , and MD5 are supported. A null value indicates that the system does not hash the password. Unless the LDAP server performs hashing (Netscape Directory Server and iPlanet Directory Server perform hashing), this will result in plaintext passwords being stored in AD.
Preferentially process the change of the resource password policy after reset	If this resource is specified in the login module (i.e., this resource is the password verification target) and the password policy of the resource is configured to change after reset, users who have reset the resource account password for management purpose need to change the password after successful verification.
Use VLV Controls	Specifies whether to forcibly use the VLV control on the standard AD control. The default value is false .
VLV Sort Attribute	Sorting attribute used for VLV indexes on resources.

Parameter	Description
Read Schema	If the value is TRUE , the connector reads the schema from the server. If FALSE , the connector provides a default schema based on the object class in the configuration. To use the extended object class, this attribute must be set to TRUE .
Basic Contexts to Synchronize	One or more starting points in the AD tree that are used to determine whether changes should be synchronized. If this attribute is not set, the base context attribute is used to synchronize changes.
Object Class to Synchronize	Object class to be synchronized. The change log is for all objects; it filters updates based on the listed object classes. You should not list the superclasses of an object class unless you want to synchronize the object with any superclass value. For example, if only the "inetOrgPerson" object should be synchronized, but the superclasses ("person", "organizationalperson", and "top") of "inetOrgPerson" should be filtered out, only "inetOrgPerson" should be listed here. All objects in AD are derived subclasses of "top". Therefore, "top" should never be listed. Otherwise, no object can be filtered.
Attribute to Synchronize	Name of the attribute to be synchronized. When this option is set, if updates in the change log do not update any named attributes, these updates are ignored. For example, if only "department" is listed, only changes that affect "department" are processed and all other updates are ignored. If you leave it blank (default setting), all changes are processed.

Parameter	Description
AD Filter for Accounts to Synchronize	Optional AD filter used during object synchronization. Because the change log applies to all objects, this filter updates only the objects that meet the specified filter criteria. If a filter is specified, the object is synchronized only when the object meets the filter conditions and contains the synchronized object class.
Change Log Block Size	Number of change log entries obtained by each query.
Change Number Attribute	Change the number attribute.
Filter with Or Instead of And	Typically, the filter used to obtain change log entries is to retrieve change entries over a period of time based on the AND condition. If this attribute is set, the OR condition will be used as the filter for the required number of changes.
Remove Log Entry Object Class from Filter	If this attribute is set (default), the filter used to obtain change log entries will not contain the "changeLogEntry" object class because the change log should not contain entries of other object classes.
Password Attribute to Synchronize	Name of the password attribute to be synchronized.
Status Management Class	Used to manage the enabling/disabling status. If no class is specified, identity status management cannot be performed.
Whether to search for passwords	Indicates whether to retrieve the user password during search. Default value: No .
DN attribute	DN attribute name of an item. The default value is entryDN .

Parameter	Description
AD Filter	An optional AD filter that controls the groups returned from AD resources. If no filter is specified, only groups containing all specified object classes are returned.
Read Timeout (ms)	Time for waiting for a response. If no response is received within the specified time, the read attempt is aborted. If the value is 0 or less than 0, there is no limit.
Connection Timeout (ms)	Waiting time for opening a new server connection. The value 0 indicates that the TCP network timeout will be used, which may be several minutes. If the value is less than 0, there is no limit.
Account DN Prefix	The default value is cn . You can also set it to another attribute name used as the DN prefix, such as uid .

- **Advanced Settings:** Policies for mapping higher-level organizations, organizations, and users.

Table 4-6 Advanced settings

Parameter	Description
Enable timer for recycling	You can set whether to enable scheduled reclamation. If scheduled reclamation is enabled, the reclamation task is executed at a specified time every day.
Timer frequency	Fixed: one day NOTE Displayed when scheduled reclamation is enabled.
Select a recycling start time	You can set the reclamation start time in the drop-down list box. NOTE This parameter needs to be set only when scheduled reclamation is enabled.
Organization	Parent organization in OneAccess to which organizations will be synchronized from AD. A new top-level organization will be automatically created if this parameter is not set.

Parameter	Description
Organization Matching	Mapping between the enterprise AD and OneAccess organizations. This policy is used when OneAccess synchronizes organizations from the enterprise AD. For example, OneAccess has an organization attribute Code and your AD has a similar attribute Organization Code . Organizations in your AD will be mapped to OneAccess, and their codes in the AD will be identified as organization codes in OneAccess.
Create Organization	Enabled by default, indicating that OneAccess will automatically create organizations that do not match any organizations in OneAccess. To ensure data integrity, enable this option.
Update Organization	Enabled by default, indicating that organizations in OneAccess that match those synchronized from the identity source will be updated. To ensure data accuracy, keep this option enabled.
Delete Organization	After organization data is synchronized from the AD to OneAccess, if you want to delete organizations from the AD, OneAccess compares the number of deleted organizations with the configured deletion threshold. If the ratio of the number of deleted organizations to the total number of data records synchronized last time is greater than the threshold, the deletion fails; if the ratio of the number of deleted organizations to the total number of data records synchronized last time is less than the threshold, the deletion is successful.
User Matching	Mapping between an AD user and a OneAccess user. Used when OneAccess synchronizes users from the enterprise AD. For example, OneAccess has a user attribute User ID and your AD has a similar attribute Employee ID . Users in your AD will be mapped to OneAccess, and their employee IDs in the AD will be identified as user IDs in OneAccess.
Create User	Enabled by default, indicating that OneAccess will automatically create users who do not match any users in OneAccess. To ensure data integrity, enable this option.
Update User	Enabled by default, indicating that users in OneAccess that match those synchronized from the identity source will be updated. To ensure data accuracy, keep this option enabled.

Parameter	Description
Delete User	After AD user data is successfully synchronized to OneAccess, if you want to delete a user from AD, OneAccess compares the number of deleted users with the configured deletion threshold. If the ratio of the number of deleted users to the total number of users synchronized last time is greater than the threshold, the deletion fails; if the ratio of the number of deleted users to the total number of data records synchronized last time is less than the threshold, the deletion is successful.
Disable User Threshold Adjustment	The default value is 20%. This is a customizable protection mechanism provided by the platform. When the number of data records disabled or deleted by the upstream identity source application exceeds the threshold, the platform will not disable or delete the data synchronously after receiving the instruction.

Step 3 (Optional) Set the object models.

Click the **Object Models** tab on the identity source details page. Then add, modify, or delete users and organization attributes and mapping rules.

Table 4-7 Object model

Parameter		Description
User	Attributes	User attributes in the AD identity source.
	Mappings	Data conversion rules for synchronizing user data from AD to OneAccess. Script-based conversion is supported.
Organization Object	Attributes	Organization attributes in the AD identity source.
	Mappings	Data conversion rules for synchronizing organization data from AD to OneAccess. Script-based conversion is supported.

- Add an attribute.
 - a. On the **Attribute** tab page, click **Add**. The **Add Attribute** dialog box is displayed.

Add Attribute ✕

*** Identity Source** --Select-- ▾

Optional Properties ?

Field Name

Description

*** Type** --Select-- ▾

Required

- b. Select the optional attributes of the identity source, and enter the display tag and description.
- c. Select a type. When **Type** is set to **Text**, you need to set **Format**.
- d. Set whether the attribute is mandatory and click **OK**. The attribute is added.
- Set the mapping rule.
On the **Mapping Definition** tab page, click **Modify**. Set the conversion mode, script expression mode, execution mode, and system user for the mapping rule.

Application Accounts	Execution Method	Conversion	Script Expression	System User
username	Create	Auto		Username
name	Create and Update	Auto		Name
organizationId	Create and Update	Auto		Organization

----End

4.2.6 Managing User Attributes

When an enterprise needs to configure more user information and synchronize it to downstream application systems, you can add and define user attributes. You can set user attributes in the basic information and work information and add custom groups as needed.

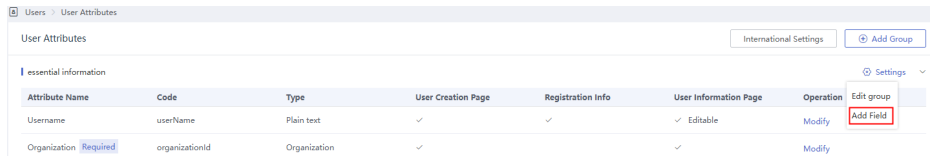
- Basic information: personal attributes, such as username and mobile number. The configured basic attributes cannot be deleted but only added or modified.
- Work information: work attribute, employee ID, and work location. The configured work information can be added or modified but cannot be deleted.

Adding Basic User Information

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > User Attributes**.

Step 3 On the user attribute definition page, choose **Settings > Add Field** on the right of **Basic Information**.



Step 4 On the page for adding a field, enter the field information.

Table 4-8 Field information and content

Parameter	Description
* Attribute Name	The attribute name must be unique.
* Code	The attribute code must be unique.
* Type	<p>Options vary depending on the attribute type.</p> <p>NOTE</p> <ul style="list-style-type: none"> If you set Type to Dictionary, select a dictionary. For details about how to add a dictionary, see Dictionaries. If Display Type is set to Sensitive text, the system anonymizes some sensitive text by default. You can select All.
Field Remarks	Description of the attribute.
Field Validation Rules	Whether an attribute is mandatory and unique, and its length is restricted.

Table 4-9 Display settings

Parameter	Description
Administrator Portal	If you select Display in query conditions , this attribute can be used as a search criterion on the user list page.
(Administrator) Adding Users	Indicates whether to display or hide the attribute when a user is added.
Editing a User as an Administrator	Indicates whether the administrator is allowed to modify the attribute when the user information is edited.

Parameter	Description
Registration information	Indicates whether to display or hide the attribute when viewing personal information.
Personal information page	<ul style="list-style-type: none"> You can set whether to display or hide the attribute when viewing personal information. You can set whether to allow users to modify the attributes when modifying personal information.
Import/Export	Indicates whether to allow the attribute import or export when importing or exporting users.

Step 5 Click **OK**. The attribute is added and displayed in the list.

----End

Adding Work Information

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > User Attributes**.

Step 3 On the user attribute definition page, choose **Settings > Add Field** on the right of **Work Information**.

Attribute Name	Code	Type	User Creation Page	Registration Info	User Information Page	Operation	Edit group
Job number	employeeid	Plain text	✓ Editable		✓	Modify	Add Field
managerid	attrManagerid	Staff	✓ Editable		✓	Modify	

Step 4 On the page for adding a field, enter the field information.

Table 4-10 Field information and content

Parameter	Description
*Field Name	The attribute name must be unique.
* Attribute Code	The attribute code must be unique.
* Field Type	<p>Options vary depending on the attribute type.</p> <p>NOTE</p> <ul style="list-style-type: none"> If you set Type to Dictionary, select a dictionary. For details about how to add a dictionary, see Dictionaries. If Display Type is set to Sensitive text, the system anonymizes partial sensitive text by default. You can choose to anonymize all sensitive text.
Field Remarks	Description of the attribute.

Parameter	Description
Field verification rule	Whether an attribute is mandatory and unique, and its length is restricted.

Table 4-11 Display settings

Parameter	Description
Administrator Portal	If you select Display in query conditions , this attribute can be used as a search criterion on the user list page.
(Administrator) Adding Users	Indicates whether to display or hide the attribute when a user is added.
Editing a User as an Administrator	Indicates whether the administrator is allowed to modify the attribute when the user information is edited.
Registration information collection	Indicates whether to display or hide the attribute when viewing personal information.
Profile page	<ul style="list-style-type: none"> You can set whether to display or hide the attribute when viewing personal information. You can set whether to allow users to modify the attributes when modifying personal information.
Import/Export Jobs	Indicates whether to allow the attribute import or export when importing or exporting users.

Step 5 Click **OK**. The attribute is added and displayed in the list.

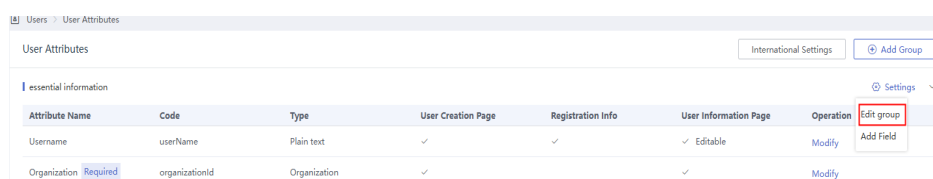
----End

Editing a Group

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > User Attributes**.

Step 3 On the user attribute definition page, choose **Settings > Add Field** on the right of **Edit Group**.



 **NOTE**

To edit a work information group, choose **Settings > Edit Group** on the right of **Work Information** on the **User Attributes** page.

Step 4 After entering the group information, click **OK**. The group information is edited. When adding a user, the administrator can add field information based on the group.

----End

Adding a Custom Group

If the basic information and work information groups cannot meet your requirements, perform the following steps to add a custom group:

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > User Attributes**.

Step 3 On the **User Attributes** page, click **Add Group**.

Step 4 Enter the group name in Chinese and English.

Step 5 Click **OK**. The group is added successfully and displayed in the group list.

----End

Deleting a Custom Group

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > User Attributes**.

Step 3 On the **User Attributes** page, choose **Settings > Delete Group** on the right of the custom group to be deleted, and click **OK** to delete the custom group.

----End

International Settings

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > User Attributes**.

Step 3 On the **User Attributes** page, click **Internationalization Settings**.

Step 4 Click **Multi-language Settings** in the **Operation** column on the right of a field to configure the field name or remarks in Chinese and English for the basic information, work information, and custom group attributes.

Step 5 Click **Save** to complete the configuration, or click **Save and Continue** to configure other Chinese and English attributes that are not configured.

----End

Deleting a Custom Attribute

NOTE

- Attributes in basic user information and work information cannot be deleted.
- Deleted custom attributes cannot be recovered. Exercise caution when performing this operation.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > User Attributes**.

Step 3 Click **Delete** in the **Operation** column of the custom attribute.

Step 4 In the displayed dialog box, click **OK** to delete the custom attribute.

----End

Modifying User Attributes

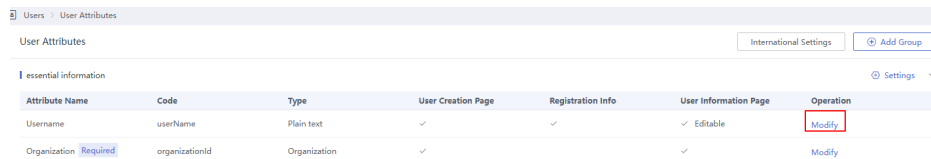
NOTE

The field name, attribute code, and field type cannot be modified.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > User Attributes**.

Step 3 Click **Modify** in the **Operation** column of the basic information, work information, or your own group list to modify user attributes.



Attribute Name	Code	Type	User Creation Page	Registration Info	User Information Page	Operation
Username	userName	Plain text	✓	✓	✓ Editable	Modify
Organization	organizationId	Organization	✓		✓	Modify

Step 4 Click **OK**. The user attributes are modified.

----End

4.2.7 Managing Authorization

With authorization management, administrators can authorize application accounts to applications and users within their scope of permissions. Users can be authorized in batches by organization, and application roles and permissions can be assigned to authorized users, in addition, you can edit, delete, enable, or disable authorized application accounts. (This function must be granted by the super administrator.)

Authorizing an Application Account

Manage the mappings between **OneAccess users** and **application accounts**. You can map a OneAccess user to accounts of different applications.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > Authorization**.

Step 3 On the displayed page, click **User Authorization** under the application to be authorized.

 **NOTE**

The **Authorization Management** page displays only the applications accessible to the administrator.

Step 4 Click **Add User** in the upper right corner. On the **Add Account** page, click the name of the organization to which the user to be authorized belongs and select it.

 **NOTE**

On the **User Authorization** page, only the application accounts on which the common administrator has permissions are displayed.

Step 5 Click **Save** to complete the authorization.

----End

Editing an Application Account

The administrator can edit the application account on the user authorization page and modify its information.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > Authorization**.

Step 3 On the page for authorization management, click **User Authorization** under an application.

Step 4 Click **Modify** in the **Operation** column of the user to modify user authorization information.

Step 5 Enter the new information and click **Save**.



----End

Disabling or Enabling an Application Account

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Users > Authorization**.

Step 3 On the page for authorization management, click **User Authorization** under an application.

Step 4 Click  in the **Status** column of the user to be disabled. After an account is disabled, the application is not displayed on the user portal of the user and it cannot be accessed. You can click  to enable the account. After the account is enabled, the application is displayed on the user portal of the user and the application can be accessed.

----End

Deleting an Application Account

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Users > Authorization**.
- Step 3** On the page for authorization management, click **User Authorization** under an application.
- Step 4** Click **Delete** in the **Operation** column of the user to be deleted.
- Step 5** In the dialog box that is displayed, click **OK** to cancel the user's permission to access the application.

----End

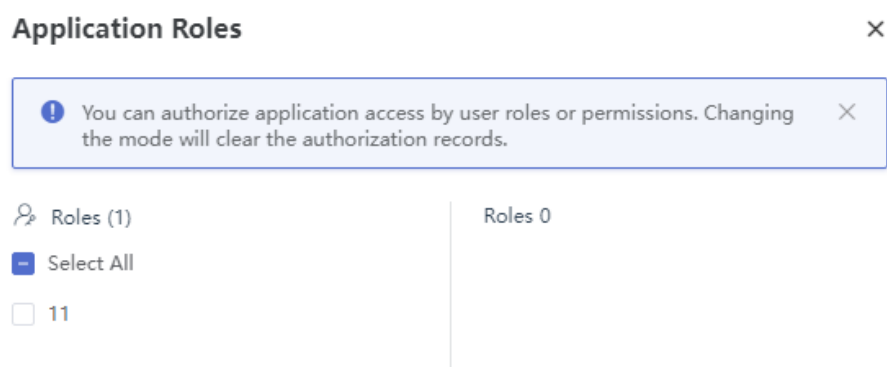
Adding an Application Role or Permission

The prerequisite for granting application roles/permissions is to configure application permissions. For details, see [Application Permission Management](#).

On the **User Authorization** page, the application accounts that the common administrator has permissions are displayed. The common administrator can add roles and permissions to these application accounts. For applications configured with role-based application permission management, you can only add roles. For applications configured with role-, permission-, and resource-based application permission management, you can add roles and permissions.

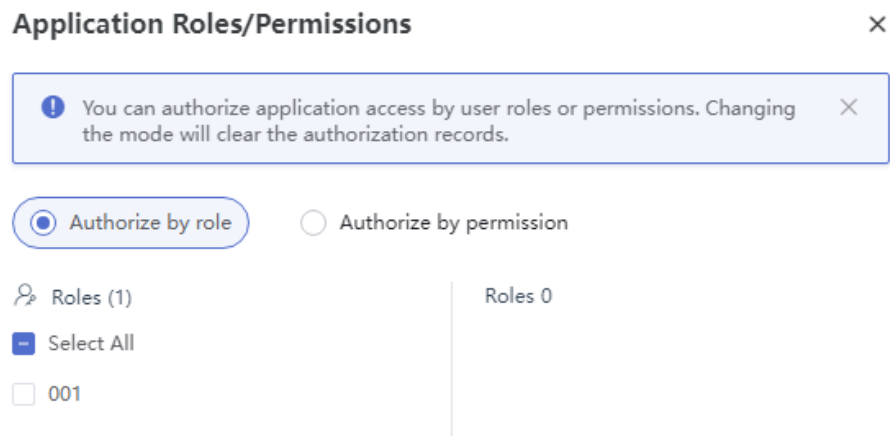
- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Users > Authorization**.
- Step 3** On the page for authorization management, click **User Authorization** under an application.
- Step 4** Click **Application Roles/Permissions** in the **Operation** column of the user to be operated.
- Step 5** Grant permissions by application role or permission.
 - The application permission of the application is set to role-based application permission management.

In the displayed dialog box, select a role name and click **OK**.

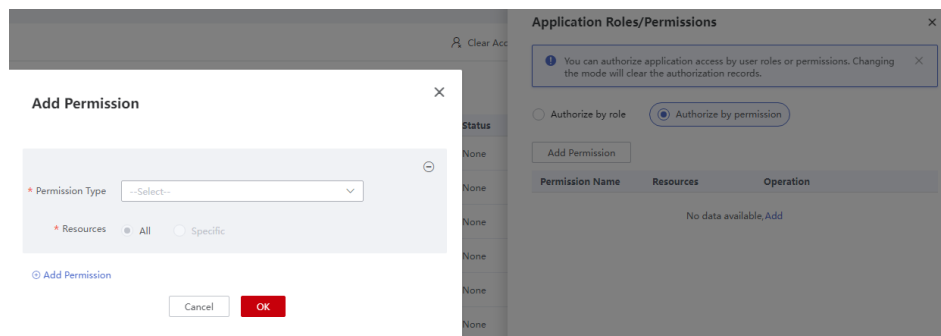


- The application permission of an application is set to role-, permission-, and resource-based application permission management.

- In the **Application Roles/Permissions** dialog box, select **Authorize by role**, select a role name, and click **OK**.



- In the **Application Roles/Permissions** dialog box, select **Authorize by permission** and click **Add Permission**. In the **Add Permission** dialog box, select a permission type, select resources, and click **OK**.

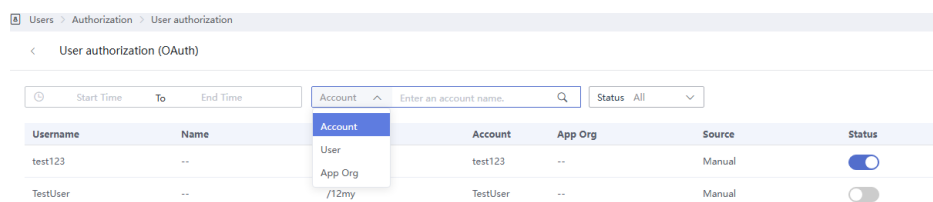


----End

Searching for an Application Account

On the **User Authorization** page, the administrator can filter application accounts based on the search criteria.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Users > Authorization**.
- Step 3** On the page for authorization management, click **User Authorization** under an application.
- Step 4** On the **User Authorization** page, you can filter users.



- You can select the start time and end time based on the application account creation time, and click **OK** to filter the application accounts created in the specified time range.
- You can select **Account** and enter an account name or name in the text box to filter application accounts that meet the search criteria.
- You can select **User** and enter an account name or name in the text box to filter application accounts that meet the search criteria.
- You can select an organization and enter the organization name or code in the text box to filter the application accounts.
- You can select **Enable** or **Disable** from the **State** drop-down list box to filter application accounts.

----End

4.3 Resources

4.3.1 Overview

You can manage applications, and enterprise APIs in a unified manner. This chapter describes how to do this with OneAccess.

Applications

Applications can be regarded as the downstream systems of an enterprise. OneAccess supports single sign-on (SSO) based on SAML, OAuth2, OIDC, and CAS. It also supports plug-in autofill and SDKs/APIs. After the configuration is complete, you can log in to the OneAccess user portal and sign in to multiple authorized applications in SSO mode. For details, see [Logging In to the User Portal and Accessing Applications](#). Data can also be synchronized from OneAccess to applications based on event callback, SCIM, and LDAP

OneAccess has pre-integrated more than 1000 applications. You can add applications as needed.

For details about application management and authorization, see [Adding an Application, Applications](#), and [Enabling, Disabling, or Deleting an Application](#).

Enterprise APIs

OneAccess supports system and custom APIs.

- System API products: built-in API products of OneAccess.
- Custom API products.

You can also register **open APIs** with OneAccess and authorize access to specific applications.

System APIs and related permissions are defined by OneAccess. Custom APIs and related permissions are defined by yourself. System APIs can only be viewed and authorized.

For details about how to authorize and call system APIs, see [Authorizing Access to Built-in APIs](#), [Calling Built-in APIs](#), [Modifying Built-in APIs](#), [Adding a Custom API](#), [Configuring a Custom API](#), and [Deleting a Custom API](#).

4.3.2 Applications

4.3.2.1 Adding an Application

OneAccess provides pre-integrated applications that you can use out-of-the-box. You can also add custom applications.

Adding a Custom Application

Custom applications are applications developed by your enterprise or any software as a service (SaaS) or commercial applications not included in the pre-integrated application list.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the **Applications** page, click **Add Custom Application**.
- Step 4** Enter an application name and its logo, and click **Save**.
- Step 5** Configure the parameters required so that the application can be accessed by users. For details, see [Applications](#).

----End

Adding a Pre-integrated Application


OneAccess has pre-integrated some applications based on their development APIs and protocols.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the **Applications** page, click **Add Pre-integrated Application**.
- Step 4** Click the pre-integrated application you want to add.
- Step 5** On the **Add Application** page, edit the general information, set the application name, and click **Next**.
- Step 6** Set the authentication parameters. The authentication integration mode and authentication parameters vary depending on the application.

SAML is used for illustration. You can upload the metadata file or manually edit metadata on the OneAccess console.

- Upload a metadata file
 - a. In the **Authentication Parameters** step, click **Import SP Metadata**.
 - b. Click **Select File** and select the metadata file you have obtained from the application service provider (SP).

 NOTE

- If a message indicating incorrect file type is displayed, upload the correct metadata file or edit the metadata manually.
- For details about how to obtain the metadata, see the documentation of the application.
- c. When the **Select File** button changes to , the metadata is extracted. Then click **Next**.
- Edit metadata
 - a. In the **Authentication Parameters** step, click **Configure Metadata**.
 - b. Set the parameters listed in the following table according to the metadata file you have obtained.

Add Application ×

1
2
3

General Information
Authentication Parameters
Finish

Parameters

Import SP Metadata

* SP Entity ID

* ACS URL

* Name ID

NameID Format

Audience URI

Single Logout URL

Relay State

Response Signature Yes No

Assertion Signature Yes No

Digital Signature Algorithm

Digital Digest Algorithm

Assertion Encryption Yes No

Previous
Next

Table 4-12 Authentication parameters

Parameter	Description
* SP Entity ID	Unique identifier of an SP. Enter the value of Entity ID displayed in the SP metadata file.

Parameter	Description
* ACS URL	SP callback URL that receives a response when OneAccess authentication is successful. Enter the value of AssertionConsumerService displayed in the SP metadata file.
* Name ID	Select a user attribute or account attribute. The attribute value will be used as the subject of the assertion.
NameID Format	Username format supported by the SP. Enter the value of NameIDFormat displayed in the SP metadata file.
Audience URI	Audience for which the SAML assertion is intended. By default, this field is the same as SP Entity ID .
Single Logout URL	URL to which users will be redirected after logging out of their sessions. Enter the value of SingleLogoutService displayed in the SP metadata file. The SingleLogoutService parameter in the metadata file must support HTTP Redirect or HTTP POST.
Relay State	Default URL to which users will be redirected after successful login.
Response Signature	This option indicates whether to sign SAML responses using the IdP's certificate.
Assertion Signature	This option indicates whether to sign assertions using the IdP's certificate. Enter the value of WantAssertionsSigned displayed in the SP metadata file.
Digital Signature Algorithm	Algorithm of SAML response or assertion signature. RSA_SHA256, RSA_SHA512, and RSA_RIPEMD160 are supported. You can select a value from the drop-down list box.
Digital Digest Algorithm	Algorithm used to create digests for SAML responses or assertions. SHA256, SHA512, and RIPEMD160 are supported. You can select a value from the drop-down list box.
Assertion Encryption	This option indicates whether to encrypt assertions.
Request Signature Validation	This option indicates whether to sign SAML requests. Enter the AuthnRequestsSigned value in the SP metadata file.
* Signature Certificate Validation	SP public key certificate, which is used to verify SAML request signatures. Enter the value of use="signing" displayed in the SP metadata file.

Step 7 Configure the synchronization parameters. The synchronization modes and parameters of different applications may be different.

Coremail is used as an example to describe how to set synchronization integration parameters.

1. Set authentication parameters and click **Next**.
2. On the synchronization configuration page, set parameters and click **Test** to test whether the configuration is correct. After the configuration is complete, click **Next**. For details about how to configure other menus, see [Applications](#).

Add Application ✕

① ——— ② ——— ③ ——— ④

General Information Authentication Parameters Synchronization Integration Finish

[Parameters](#)

Test

Basic Settings ∨

* API Request Domain ⓘ
Name

* API Request Port ⓘ



* Organization Domain ⓘ
Names

Optional >

----End

4.3.2.2 Enabling, Disabling, or Deleting an Application

Disabling or Enabling an Application

- You can disable an application on the application information page.
 - a. Log in to the administrator portal.
 - b. On the top navigation bar, choose **Resources > Applications**.
 - c. On the displayed page, click an application name to access the application details page.
 - d. Click  in the upper right corner of the page. In the dialog box that is displayed, click **OK**. Disabled applications are displayed in the **Disabled Applications** section.
- You can enable a disabled application on the app page.
 - a. Log in to the administrator portal.
 - b. On the top navigation bar, choose **Resources > Applications**.
 - c. On the application page, click **Disabled Applications**.
 - d. Click  in the upper right corner of the application to be enabled and select **Enable**.
 - e. In the dialog box that is displayed, click **OK**. The application is no longer displayed in the **Disabled Applications** section.

NOTE


Disabled applications will no longer be displayed on the user portal of the users who have been granted access to them.

Deleting an Application

NOTICE

If an application is deleted, all data of the application will be deleted and cannot be recovered.

- Delete an application that is not disabled.
 - a. On the **Applications** page, click the application you want to delete.
 - b. On the application information page, click the application logo or name to go to the information page.
 - c. Click **Delete Application**.
 - d. Enter the application name and click **OK**. The integration application is deleted.
- Delete a disabled app.
 - a. Log in to the administrator portal.
 - b. On the top navigation bar, choose **Resources > Applications**.
 - c. On the application page, click **Disabled Applications**.

- d. Click  in the upper right corner of the application to be enabled, and click **Delete Application**.
- e. In the dialog box that is displayed, click **OK**. The application is not displayed on the application page.

4.3.2.3 General Information

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 Click an application to go to the information page.

Step 4 Click the logo or name to access the general information page. On this page, view the following information:

- Authentication Credentials
 - **ClientId**: API authentication ID is automatically generated after application registration.
 - **ClientSecret**: API authentication secret is obtained by clicking **Enable** after application registration.

 **NOTE**

If the access secret is lost, click **Reset** to get a new one.


- Application
You can click **Modify** to modify the application logo and name, and then click **Save**.
- Integration
 - **Authentication Integration**: You cannot change the protocol for integrating the application with OneAccess for identity authentication once specified.
 - **Synchronization Integration**: You cannot change the method of synchronizing data between the application and OneAccess once specified.
- Other
Click **Modify** to modify the application display mode (automatic, fixed and not display) on the homepage of the user portal.
 - **Automatic**: The application is displayed only for users who have access to the application.
 - **Fixed**: The application is displayed for all users.
 - **Not display**: The application is not displayed for any users.
- Delete an application
Click **Delete Application**, and enter the application's name in the displayed box. Click **OK** to delete it.

----End

4.3.2.4 Authentication Integration

Configuring authentication integration requires **Parameters** and **Mappings**. If the integration mode is **Plug-in autocompletion**, the **Basic Settings** and **Account Settings** are required.

Configuring Parameters

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** Click an application to go to the information page.
- Step 4** On the **General Information** page, click  next to **Authentication** to access the authentication integration page, select an appropriate integration mode, and then click **Save**.
- Step 5** On the **General Information** page, click **Configure** next to **Authentication** to access the **Parameters** page, set parameters and then click **Save**. Configure the parameters based on authorization integration modes.
 - For details about the configuration of the SAML, see [Authentication Integration](#).
 - For details about the configuration of the OAuth2, see [Authentication Integration](#).
 - For details about the configuration of the OpenID Connect, see [Authentication Integration](#).
 - For details about the configuration of the CAS, see [Authentication Integration](#).
 - For details about the configuration of plug-in autocompletion, see [Authentication Integration](#).

----End

Mappings

Mapping configuration (add, edit, and delete) refers to attributes that need to be returned to the application after authentication to establish the mapping between OneAccess and the application attribute.

- **Add a mapping**
The SAML protocol is used as an example to describe how to add mappings. Click the **Mappings** and **Add Mapping** to enter details, and then click **Save**.

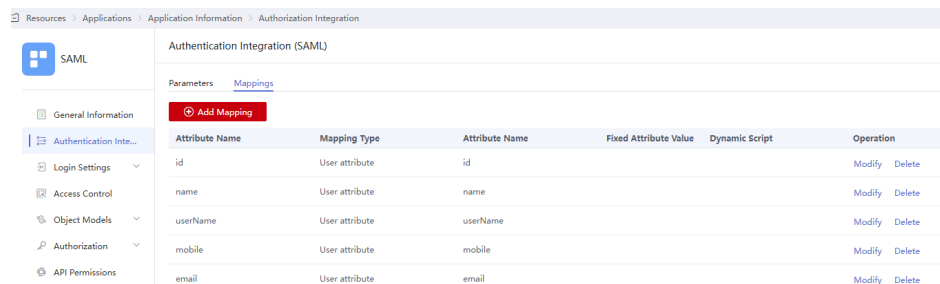


Table 4-13 Mapping parameters


Parameter	Description
* Application Attribute	User attribute of an enterprise application, which OneAccess will return to the application after authentication.
* Mapping Type	<p>Different mapping types determine the attribute values returned by the API after authentication.</p> <ul style="list-style-type: none"> • User attribute: Return the user attribute to the downstream enterprise application. • Account attribute: Return the account attribute to the downstream enterprise application. • Account permission: Return the account permission to the downstream enterprise application. If a downstream application requires permission information of OneAccess users, you can return them by this method. • Social attribute: Return the social attribute value to the downstream enterprise application. • Fixed attribute value: A fixed value can be configured. • Dynamic script: You can use a script to customize the attribute values returned to the downstream enterprise applications. For details, see Developing Mapping Scripts. • Session: The session parameters are returned to the downstream enterprise application. • Application: Add the mapping authorized to the application.
* User Attribute	Attribute mapped from OneAccess to the application. The options of the attribute vary based on the mapping type.
* Friendly Name	Enter the same value as the Application Attribute . This parameter is available when the authentication protocol is SAML.
* Attr Name Format	Format of data returned in accordance with the SAML protocol.

- Modify a mapping
Click **Modify** in the **Operation** column of the added mapping. On the **Modify Mapping** page, modify the mapping and then click **Save**.
- Delete a mapping
Click **Delete** in the **Operation** column of the added mapping and click **OK** to delete the mapping. To add again, see [Add a mapping](#).

4.3.2.5 Synchronization Integration

Configuring synchronization integration includes **Parameters** and **General**. When the integration mode is **Event callback**, the operation also includes **Full Synchronization**.

Configuring Parameters

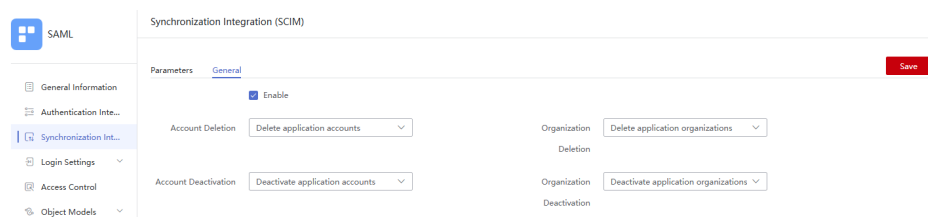
- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** Click an application to go to the information page.
- Step 4** On the **General Information** page, click  next to **Synchronization Integration** to select an appropriate integration mode, and then click **Save**.
- Step 5** On the displayed page, click **Configure** next to **Synchronization Integration** to set parameters, and then click **Save**. Configure the parameters based on synchronization integration modes.
 - For details about configuring integration parameters for event callback synchronization, see [Configuring Event Callback](#).
 - For details about SCIM-based integration parameters, see [Synchronization Configuration](#).
 - For details about LDAP synchronization parameters, see [Synchronization Configuration](#).

----End

General Configuration

General Configuration: indicates the mapping during synchronization.

On the **Synchronization Integration** page, click **General** to enable it. The configuration mapping includes deleting and disabling an account and organization.



- Delete an account
After an application account is deleted from OneAccess, the downstream application system determines the operation (deleting and disabling accounts and asynchronization) to be performed based on the configuration.
- Delete an organization
After an organization is deleted from OneAccess, the downstream application system determines the operation (deleting and disabling organizations, and asynchronization) to be performed based on the configuration.

- **Disable an account**
After an application account is disabled in OneAccess, the downstream application system determines the operation (disabling accounts, and asynchronization) to be performed based on the configuration.
- **Disable an organization**
After an organization is disabled in OneAccess, the downstream application system determines the operation (disabling organizations, and asynchronization) to be performed based on the configuration.

Full Synchronization

If the integration mode is event callback, full synchronization can be implemented. For details, see [Full Synchronization](#).

4.3.2.6 Login Configuration

OneAccess allows you to configure an independent sign-in authentication mode for each app, including official accounts, website and mobile apps.

Web Applications

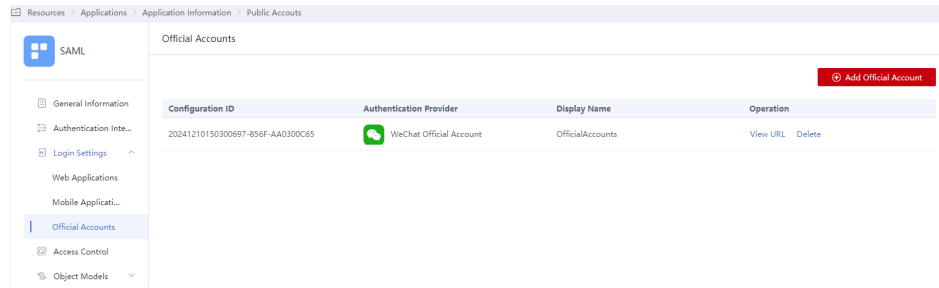
- Configure the login authentication mode for enterprise users to access applications through browsers on PCs. Before enabling authentication, you need to add an authentication provider. For details, see [Authentication Provider Integration](#).
- Only one of password, AD, and LDAP authentication can be enabled at a time.
- The configuration ID and mounting URL are automatically generated by the system. You can access the mounting URL to log in to the application through a browser. The URL can be edited.

Mobile Applications

- Configure the login authentication mode for enterprise users to access applications from mobile devices. Before enabling authentication, you need to add an authentication provider. For details, see [Authentication Provider Integration](#).
- Only one of password, AD, and LDAP authentication can be enabled at a time.
- The configuration ID and mounting URL are automatically generated by the system. You can access the mounting URL to log in to the app on the mobile device. The URL can be edited.

Official Accounts


- Configure password-free login for enterprise apps through WeChat official accounts. Before configuration, you need to add an authentication provider of WeChat official accounts.
- On the page for configuration, click **Add Official Account**, and then select an authentication provider. After the configuration is added, the system automatically generates the configuration ID and mounted URL. Click **View URL** to view the URL, and click **Delete** to delete the URL.



4.3.2.7 Access Control


You can control authorized users' behaviors through access control policies. If a user is not authorized to access an application, the policies do not take effect for the user. Before you configure custom policies, enable access control to set a default policy.

The following describes how to configure a custom policy.


- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** In the **General Information** area, click  next to **Authentication**, select an authentication mode, and click **Save**.

 **NOTE**


Enable **Authentication** before you configure access control.

- Step 5** In the **General Information** area, click **Configure** in the row that contains **Authentication** to access the **Authentication Integration** page.
- Step 6** In the navigation pane on the left, choose **Access Control**. On the displayed page, click  in the upper right corner. On the displayed page, configure the default policy.


 **NOTE**

To disable the default policy, click . Exercise caution when performing this operation, since all policies will be deleted and cannot be recovered.

Enable Access Control ×

 Configure the default access control policy to control access of users who do not match any custom policies. ×

- Default Policy Allow access of all users Deny access of all users
 MFA authentication

Step 7 Click **Save**. The added default policy is displayed on the access control page. To modify the default policy, click  next to it. In the displayed window, modify the default policy.

Step 8 On the access control page, click **Add Policy**, set parameters, and click **Save**.

Add a strategy
✕

*** Policy Name**

Description

IF User Condition

AND Access Time

AND Device Type

AND Regions

AND Authentication Provider

THEN Allow Deny MFA authentication

*** Frequency** Upon login Every session

*** Authentication** OTP SMS EMAIL FIDO2(WebAuthn)

Method Fingerprint (WeChat mini program)

Table 4-14 Policy parameters

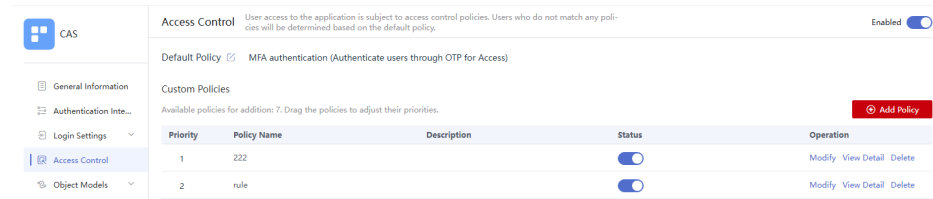
Parameter	Description
* Policy Name	Name of a policy.
Description	Description of a policy.
User Condition	Users who can or cannot access the application. You can select a condition from the drop-down list box.
Condition Type	Method of determining the user access conditions (User Group , Organization , Users , and Custom Condition).
User Group	Group of users who are allowed or disallowed to access the application. For details, see Managing User Groups .

Parameter	Description
Organization	Organization with users who are allowed or disallowed to access the application. For details, see Managing Organizations .
Users	Users who are allowed or disallowed to access the application. For details, see Managing Users .
Custom Condition	<ul style="list-style-type: none"> Attributes used to define users who are allowed or disallowed to access the application. For details, see Managing User Attributes. To add more custom conditions, click Add Custom Condition.
Access Time	Select the time frame during which the application can be accessed.
Date	Select the date on which the application can be accessed.
Period	Select the time period during which the application can be accessed.
Specific periods	<ul style="list-style-type: none"> Specify a time period to control user access behaviors. To add more time periods, click Add Period.
Device Type	<p>Type of devices that are allowed or not allowed to access the application. The options include Browser, Desktop device, and Mobile device.</p> <ul style="list-style-type: none"> Browser: Google Chrome, Firefox, Internet Explorer, and other Desktop device: Windows, Linux, macOS, and other Mobile device: Android, iOS, and other
Regions	<ul style="list-style-type: none"> Select the region where the application can be accessed. You can also specify regions by referring to Managing Regions.
Authentication Provider	Select the authentication provider for accessing the application.
THEN	<p>Whether to allow access to the application. If you select MFA authentication, set the following parameters:</p> <ul style="list-style-type: none"> Frequency: Specify the frequency for accessing an application with the MFA authentication. Authentication Method: Specify a method. After OTP is selected, users can obtain the OTP as prompted. For details about the configuration, see Configuring OTP. If you select multiple authentication methods, users can select one of these MFA methods during the login process.

----End

If you configure multiple application access control policies, you can adjust their priorities. When an enterprise user accesses an application, custom policies are

used based on their priorities. If no custom policies are matched, the default policy is used to determine whether the user can access the application.



- You can drag and drop policies in the list to adjust their priorities.
- Click **Modify** in the **Operation** column of a policy. On the displayed page, modify the policy configuration and click **Save**.
- Click **View Details** in the **Operation** column of a policy to check its information.
- Click **Delete** in the **Operation** column of a policy. In the displayed dialog box, click **OK** to delete the policy.

4.3.2.8 Object Models

Object models, including the application account model and application organization model, are the basis for synchronizing data from OneAccess to downstream applications.

After synchronization is enabled, common attributes such as the account name, name, and application organization are defined by OneAccess. To synchronize more attributes, add attributes and configure mappings through the object model. The added attribute name must be the same as that of the application. In addition, You can set the status of an application account or organization after the system user or organization is deleted or disabled.

Application Accounts

- Attributes
 - a. Log in to the administrator portal.
 - b. On the top navigation bar, choose **Resources > Applications**.
 - c. On the displayed page, click an application name to access the application details page.
 - d. Click the application icon to access the general information page.
 - e. In the navigation pane on the left, choose **Object Models > Application Accounts**. On the displayed **Attributes** tab page, click **Add**, configure the application account attribute, and click **Save**.

Add Attribute ×

* Attribute

* Label

Description

* Attribute Type Please select attribute type ▼

Required
 Unique
 Sensitive

Table 4-15 Attribute parameters

Parameter	Description
* Attribute	Attribute name of an application account.
* Label	Identifier of an attribute. It is recommended that the value of this parameter be matched with that of Attribute .
Description	Description of Attribute .
* Attribute Type	Type of an attribute. You can select a value from the drop-down list box.
Format	This parameter specifies the text format. It is required only when Attribute Type is set to Text .
Required	If this option is selected, the attribute must be set when user data is synchronized to the application. If the attribute is left empty, a message will be displayed, indicating that label is mandatory.
Unique	It is required only when Attribute Type is set to Text . If this option is selected, the attribute value must be unique when user data is synchronized to the application. If the attribute value is duplicate, a message is displayed, indicating that the label already exists.
Sensitive	It is required only when Attribute Type is set to Text . If this option is selected, the data is hidden when user data is synchronized to the application. You can click to check the data.

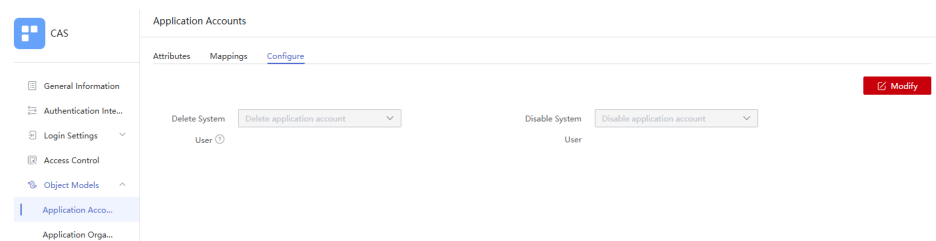
- f. You can click **Modify** or **Delete** in the **Operation** column on the right to edit or delete an attribute. Built-in attributes cannot be deleted.

- Mappings
Go to the **Mappings** tab page, click **Modify**, and configure account attribute mappings. To prevent synchronization exceptions, you are advised to add account attributes of the same type as the user attributes to be mapped.

Table 4-16 Mapping parameters

Parameter	Description
User	User attribute mapped to the Application Account . You can select a value from the drop-down list box.
Conversion Mode	Mode of attribute mapping between User and Application Account .
Script Expression	Enter the mapping script. For details, see Developing Mapping Scripts .
Execution Mode	Synchronization mode of the Application Account attribute. You can select a value from the drop-down list box.
Application Account	Label of the application account attribute.

- Configuration
Click the **Configure** tab. By default, **Delete System User** is set to **Delete application account**, and **Disable System User** is set to **Disable application account**. Click **Modify** to modify the configuration. If you choose to disable or retain the application account for **Delete System User**, the account automatically changes to an orphan account because the user has been deleted. You can choose to retain an application account for **Disable System User**. Click **Save** to make the modification take effect.




Application Organizations

Before configuring the application organization, you need to enable it. The configuration method is similar to that of the application account. For details, see [Application Accounts](#).

To prevent synchronization exceptions, you are advised to add organization attributes of the same type as the application organization attributes to be mapped.

- Attributes
 - a. Log in to the administrator portal.

- b. On the top navigation bar, choose **Resources > Applications**.
- c. On the displayed page, click an application name to access the application details page.
- d. Click the application icon to access the general information page.
- e. In the navigation pane on the left, choose **Object Models > Application**

Organization. On the displayed page, click . In the displayed dialog box, click **OK** to enable the application organization. On the displayed **Attributes** tab page, click **Add**, configure the application organization attribute, and click **Save**.

Add Attribute ×

* Attribute

* Label


Description

* Attribute Type

Required
 Unique
 Sensitive

Table 4-17 Attribute parameters

Parameter	Description
* Attribute	Attribute of an application organization.
* Label	Identifier of an attribute. It is recommended that the value of this parameter be matched with that of Attribute .
Description	Description of Attribute .
* Attribute Type	Type of an attribute. You can select a value from the drop-down list box.
Format	This parameter specifies the text format. It is required only when Attribute Type is set to Text .
Required	If this option is selected, the attribute must be set when organization data is synchronized to the application. If the attribute is left empty, a message will be displayed, indicating that label is mandatory.

Parameter	Description
Unique	It is required only when Attribute Type is set to Text . If this option is selected, the attribute value is unique when organization data is synchronized to the application. If the attribute value is duplicate, a message is displayed, indicating that the label already exists.
Sensitive	It is required only when Attribute Type is set to Text . If this option is selected, the data is hidden when organization data is synchronized to the application. You can click  to check the data.

You can click **Modify** or **Delete** in the **Operation** column on the right to edit or delete an attribute. Built-in attributes cannot be deleted.

- Mappings

Go to the **Mappings** tab page, click **Modify**, and configure account attribute mappings. To prevent synchronization exceptions, you are advised to add account attributes of the same type as the user attributes to be mapped.

Table 4-18 Mapping parameters

Parameter	Description
Organization	Organization attribute mapped to the application organization. You can select a value from the drop-down list box.
Conversion Mode	Mode of attribute mapping between Organization and Application Organization .
Script Expression	Enter the mapping script. For details, see Developing Mapping Scripts .
Execution Mode	Synchronization mode of the Application Organization attribute. You can select a value from the drop-down list box.
Application Organization	Label of the application organization attribute.

- Configuration

Click the **Configure** tab. By default, **Delete System Org** is set to **Delete application organization**, and **Disable System Org** is set to **Disable application organization**. You can click **Modify** to modify the configuration. You can set **Delete System Org** to **Disable application organization** or **Do not affect**, and set **Disable System Org** to **Do not affect**. Click **Save** for the modification to take effect.

4.3.2.9 Authorization Management

4.3.2.9.1 Managing Application Accounts

You can manage the mappings between OneAccess users and application accounts. That is, you can map a OneAccess user to accounts of different applications.

If synchronization parameters have been configured and the synchronization is normal, adding, deleting, editing, enabling, and disabling application accounts through authorization policies will trigger the synchronization to downstream applications. For details, see [Synchronizing Data to Applications Through Event Callback](#).

Application accounts include new accounts and existing accounts.

- **New accounts**
New accounts are assigned accounts. You can grant enterprise users the permission to access applications by manually adding accounts or through authorization policies.
- **Existing accounts**
Existing accounts are bound accounts. If OneAccess users are bound to existing accounts, you can import these existing accounts to application accounts. Or, you can import existing accounts to orphan accounts, then bind OneAccess user to these existing accounts. For details, see [Application Accounts](#).

Adding Accounts

You can manually grant application permissions to users by adding accounts. If automatic authorization is required, see [Configuring Authorization Policies for Application Accounts](#).

If automatic authorization is enabled for application organizations, you can select only automatically authorized organizations when adding an account. For details, see [Configuring Authorization Policies for Application Organizations](#).

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 Click the application icon to access the general information page.

Step 5 In the navigation pane on the left, choose **Authorization > Application Accounts** to access the application accounts page.

Step 6 Click **add Accounts**. On the displayed page, select the users to whom you want to grant application permissions, and click **Save**.

----End

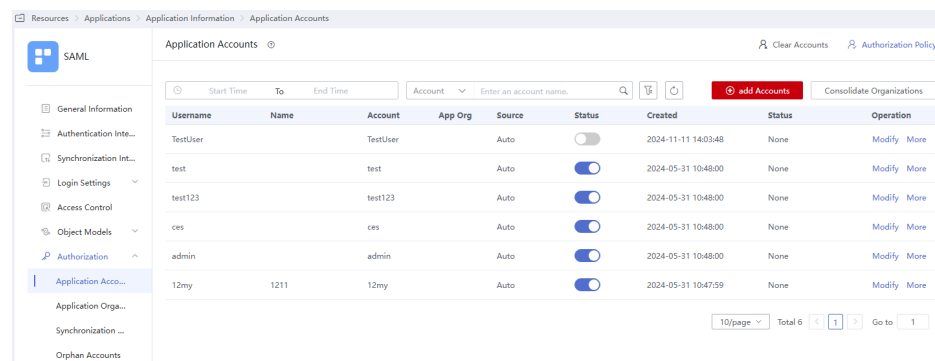
Consolidating User Organizations

If automatic authorization is enabled and no organization mapping is set for the application account model, you can click **Consolidate Organizations** to show the

application organization to which the application account belongs in the account list. For details about automatic authorization, see [Configuring Authorization Policies for Application Organizations](#). For details about application account model configuration, see [Application Accounts](#).

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Application Accounts**.
- Step 6** Click **Consolidate Organizations**.

Figure 4-4 Consolidating user organizations



Username	Name	Account	App Org	Source	Status	Created	Status	Operation
TestUser		TestUser		Auto	<input type="checkbox"/>	2024-11-11 14:03:48	None	Modify More
test		test		Auto	<input checked="" type="checkbox"/>	2024-05-31 10:48:00	None	Modify More
test123		test123		Auto	<input checked="" type="checkbox"/>	2024-05-31 10:48:00	None	Modify More
ces		ces		Auto	<input checked="" type="checkbox"/>	2024-05-31 10:48:00	None	Modify More
admin		admin		Auto	<input checked="" type="checkbox"/>	2024-05-31 10:48:00	None	Modify More
12my	1211	12my		Auto	<input checked="" type="checkbox"/>	2024-05-31 10:47:59	None	Modify More

----End

Clearing Accounts

If you clear accounts, the authorization data of the application will be initialized. This means that the application access permissions granted to authorized users will be cancelled.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Application Accounts** to access the application accounts page.
- Step 6** Click **Clear Accounts**.

NOTE

In the displayed dialog box, if you select **Delete all orphan accounts and shared accounts**, the orphan accounts and shared accounts will be cleared. After the shared accounts are cleared, they will not be displayed in the shared account list.

Step 7 Click **OK**.

----End

Configuring Authorization Policies for Application Accounts

Users' permissions to access applications can be automatically granted and deleted through authorization policies. This allows you to manage user permissions in a unified manner.

After automatic user authorization is enabled, any actions performed on an authorized organization, such as adding and deleting users, adjusting user organizations, as well as adding and deleting users within an authorized user group, can be automatically synchronized to the applications.

Step 1 Log in to the administrator portal.

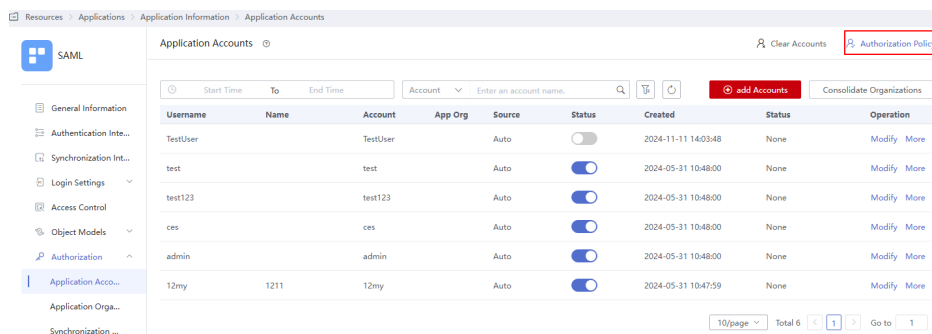
Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.


Step 4 Click the application icon to access the general information page.

Step 5 In the navigation pane on the left, choose **Authorization > Application Accounts** to access the application accounts page.

Step 6 Click **Authorization Policy**.




Username	Name	Account	App Org	Source	Status	Created	Status	Operation
TestUser		TestUser		Auto	<input type="checkbox"/>	2024-11-11 14:03:48	None	Modify More
test		test		Auto	<input checked="" type="checkbox"/>	2024-05-31 10:48:00	None	Modify More
test123		test123		Auto	<input checked="" type="checkbox"/>	2024-05-31 10:48:00	None	Modify More
ces		ces		Auto	<input checked="" type="checkbox"/>	2024-05-31 10:48:00	None	Modify More
admin		admin		Auto	<input checked="" type="checkbox"/>	2024-05-31 10:48:00	None	Modify More
12my	1211	12my		Auto	<input checked="" type="checkbox"/>	2024-05-31 10:47:59	None	Modify More


Step 7 On the **Authorization Policy** page, click  to enable automatic user authorization, select users, and click **Save** to save the current policy.

NOTE

- When automatic authorization is enabled for an application organization and users in all organizations or custom users are selected, the organization scope is limited to automatically authorized organizations. In this case, users in these organizations can be granted the permission to access the application. However, the user group scope is not restricted by automatic organization authorization. For details, see [Configuring Authorization Policies for Application Organizations](#).
- After a disabled user is enabled again, automatic authorization will not be triggered. You need to manually authorize the user.
- If you select all users in the organizations, all organizations are displayed, indicating that all users are granted the permission to access the application.
- When **Users** is set to **Custom**:

- If the condition is set to **AND**, you can select either or both of the organization and user group. In this case, users in the selected organizations, user groups, or both will be granted the permission to access applications.
- If the condition is set to **OR**, you need to select both the organizations and user groups to grant all users in the selected organizations and user groups the permission to access applications.

Step 8 Click **Add** to complete user authorization. Click  to make the selected user displayed in the application account list.

Step 9 If you want to cancel organization-based and user group-based authorization in batches, deselect the organizations and user groups to be deleted on the authorization policy page and click **Save**. The current policy is saved but user authorization will not be canceled immediately. Click **Delete** to cancel the authorization. After the deletion, click . The user whose authorization has been canceled is not displayed in the application account list.

----End

Modifying an Account

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 Click the application icon to access the general information page.

Step 5 In the navigation pane on the left, choose **Authorization > Application Accounts** to access the application accounts page.

Step 6 Click **Modify** in the **Operation** column of the application account to modify user authorization information. The account attributes displayed on this page can be configured based on the attribute definition of the application account. For details, see [Application Accounts](#).

Step 7 Click **Save**.

----End

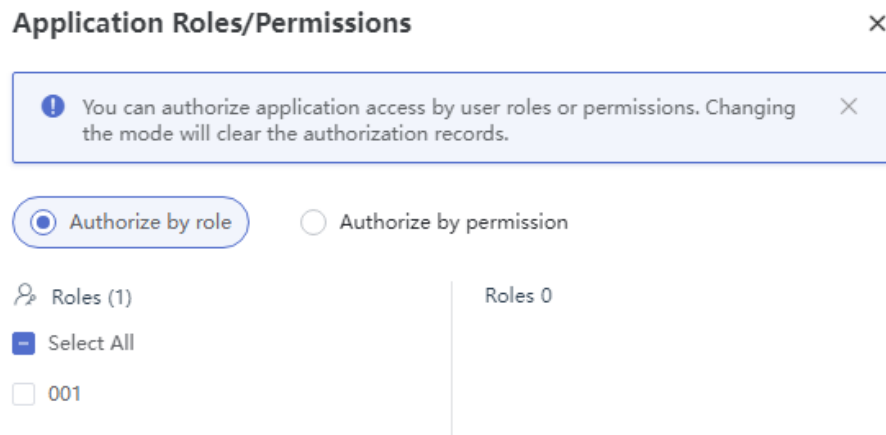
Application Roles and Permissions

The prerequisite for granting application roles/permissions is to configure application permissions. For details, see [Application Permission Management](#).

On the application account page, choose **More > Application Roles/Permissions** in the **Operation** column.

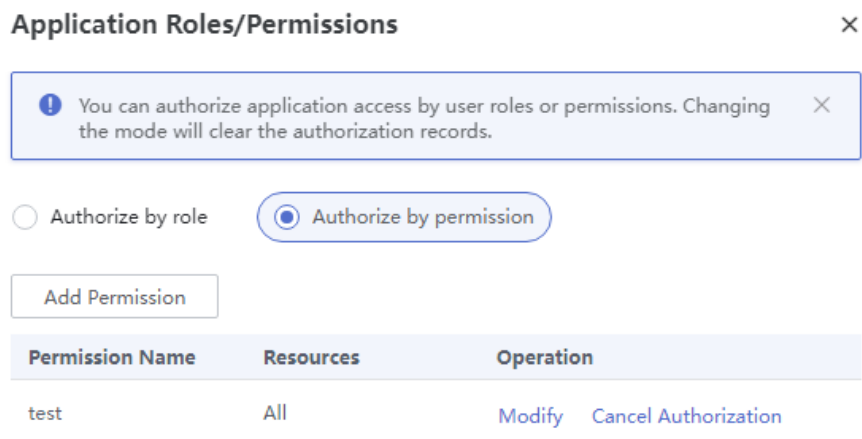
- If you choose to authorize application permissions by role, you can grant permissions only by application role. Select the account to which the role is to be granted and click **OK**. For details, see [Managing Permissions by Roles](#).

Figure 4-5 Granting permissions by role

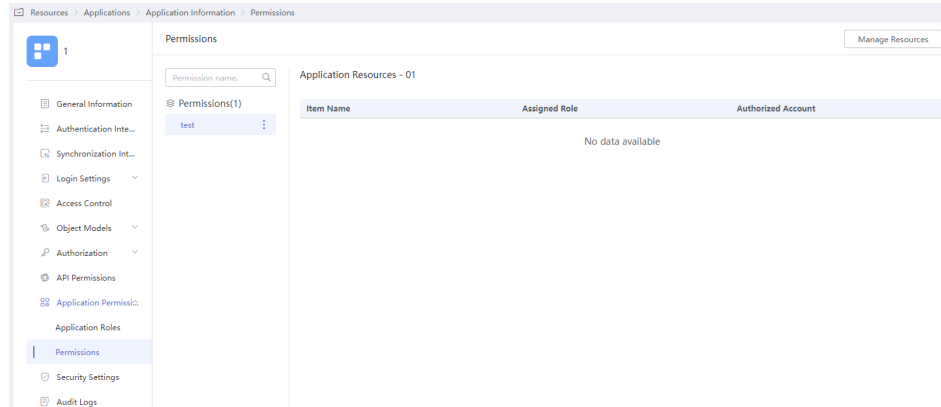


- If you choose to manage application authorization based on roles, permissions, and resources, you can authorize permissions by application role or by application permission. Only one authorization mode can be selected for each account.
 - Click **Authorize by permission** and click **Add Permission**. On the displayed page, select a permission type, select all resources or specify desired resources, and click **OK**. Resource items and their subitems have separate permissions that need to be granted individually.

Figure 4-6 Granting permissions by role



After you grant permissions by application permission, you can choose **Application Permissions > Permissions** to view the permissions in the authorized account.



- For details about authorizing permissions by role, see [Granting Permissions by Role](#).

Transferring To an Orphan Account

- Step 1** Log in to the administrator portal.
 - Step 2** On the top navigation bar, choose **Resources > Applications**.
 - Step 3** On the displayed page, click an application name to access the application details page.
 - Step 4** Click the application icon to access the general information page.
 - Step 5** In the navigation pane on the left, choose **Authorization > Application Accounts** to access the application accounts page.
 - Step 6** In the **Operation** column of the target application account, choose **More > Transfer to orphan account**.
 - Step 7** Click **OK**. The transferred account is displayed on the **Authorization > Orphan Accounts** page.
- End

Deleting an Account

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Application Accounts** to access the application accounts page.
- Step 6** In the **Operation** column of the target application account, choose **More > Delete**.

Step 7 In the displayed dialog box, click **OK**. After an authorized account is deleted, the account no longer has the permissions to access the application. For details about batch deletion, see [Configuring Authorization Policies for Application Accounts](#).

----End

Enabling or Disabling an Account


Step 1 Log in to the administrator portal.


Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 Click the application icon to access the general information page.

Step 5 In the navigation pane on the left, choose **Authorization > Application Accounts** to access the application accounts page.

Step 6 On the application account page, click  in the **Status** column to disable an account. After the account is disabled, the application is not displayed on the user portal of the user.

Step 7 Click  in the **Status** column to enable the account. After the account is enabled, the application is displayed on the user portal, allowing users to access it. For details about how to access an application, see [Logging In to the User Portal and Accessing Applications](#).

----End

4.3.2.9.2 Managing Application Organizations

Application organizations help manage the relationship between applications and OneAccess organizations. The following scenarios are involved:

- The organizations of an application are the same as that of OneAccess. They synchronize with OneAccess.
- The organizations of an application are part of OneAccess. They synchronize with OneAccess.
- The organizations of an application consist of all or part of OneAccess. Each application has its own virtual organization.

Enable application organizations before using them. For details, see [Application Organizations](#).

If synchronization parameters have been configured and the synchronization is normal, adding and deleting application organizations as well associated adding, editing, moving, and deleting virtual organizations through authorization policy will trigger the synchronization to downstream applications. For details, see [Synchronizing Data to Applications Through Event Callback](#).

Application organization allows you to clear organizations, set authorization policies, as well as add, edit, move, and delete virtual organizations.

Clearing Organizations

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Application Organizations** to access the application organizations page.
- Step 6** Click **Clear Organizations**. In the displayed dialog box, click **OK**. The organizations of OneAccess are cleared. This operation is not synchronized to the downstream applications.


NOTE



- After organizations are cleared, you can select all organizations in OneAccess when you add accounts or grant permissions to users.
- If the application account, orphan account, and shared account of an authorized organization are not cleared, you need to clear them first before you clear the organization.

----End

Configuring Authorization Policies for Application Organizations

If synchronization parameters have been configured and the synchronization is normal, adding, editing, moving, and deleting sub-organizations for application organizations (added through authorization policy) will trigger synchronization to downstream applications. For details, see [Managing Organizations](#).


- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Application Organizations** to access the application organizations page.
- Step 6** Click **Authorization Policy**.
- Step 7** On the **Authorization Policy** page, click  to enable automatic organization authorization and click **Save** to save the current policy.
 - If you select all organizations, all organizations in OneAccess will be authorized.
 - If you select custom organizations, you need to select at least one organization. If you do not enable parent organization synchronization, only the selected organizations are authorized. If you enable this function, the parent organizations of the selected organizations are also authorized.

- Step 8** Click **Add** to complete organization authorization. Then, click , the selected organization is displayed in the application organization list.
- Step 9** If you want to delete authorized organizations in batches, deselect the organizations to be deleted on the authorization policy page and click **Save**. The current policy is saved but organization authorization will not be canceled immediately. Click **Delete** to cancel the authorization. After the deletion, click . The organization whose authorization has been canceled is not displayed in the application organization list.

----End

Adding a Virtual Organization

Virtual organizations belong to enterprise applications. They are independent organizations of enterprise applications.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Application Organizations** to access the application organizations page.
- Step 6** Click . On the displayed **Add Virtual Organization** page, enter an organization name and code, and select a parent organization.
- Step 7** Click **Save**. The virtual organization is added. If you select a parent organization, the added virtual organization is a sub-organization. If you do not select a parent organization, the added virtual organization is the top-level organization.

----End

Modifying a Virtual Organization

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Application Organizations** to access the application organizations page.
- Step 6** Click **Modify** in the **Operation** column of a virtual organization to modify its information.

----End

Moving a Virtual Organization

- Step 1** Log in to the administrator portal.
 - Step 2** On the top navigation bar, choose **Resources > Applications**.
 - Step 3** On the displayed page, click an application name to access the application details page.
 - Step 4** Click the application icon to access the general information page.
 - Step 5** In the navigation pane on the left, choose **Authorization > Application Organizations** to access the application organizations page.
 - Step 6** Click **Move** in the **Operation** column of a virtual organization to modify its parent organization.
- End

Deleting a Virtual Organization

- Step 1** Log in to the administrator portal.
 - Step 2** On the top navigation bar, choose **Resources > Applications**.
 - Step 3** On the displayed page, click an application name to access the application details page.
 - Step 4** Click the application icon to access the general information page.
 - Step 5** In the navigation pane on the left, choose **Authorization > Application Organizations** to access the application organizations page.
 - Step 6** Click **Delete** in the **Operation** column of the target virtual organization.
 - Step 7** In the displayed dialog box, click **OK**. For details about how to add a virtual organization again, see [Adding a Virtual Organization](#).
- End

4.3.2.9.3 Managing Synchronization Events

When OneAccess synchronizes data to downstream applications, all synchronization operations are recorded.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Synchronization Events** to access the synchronization events page. You can filter synchronization records by time, operation type, object type, and synchronization status.

 **NOTE**

If synchronization failed:

- View the response and resolve the issue, and then try again.
- Click **Retry** to quickly perform synchronization. After you successfully retry the synchronization event of the parent organization, the synchronization events of the sub-organizations and accounts under the parent organization will be triggered.

----End

4.3.2.9.4 Managing Orphan Accounts

An orphan account is an account that is not bound to any OneAccess user.

If synchronization parameters have been configured and the synchronization is normal, adding, editing, and deleting orphan accounts will trigger synchronization to downstream applications. For details, see [Synchronizing Data to Applications Through Event Callback](#).

Adding Accounts

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 Click the application icon to access the general information page.

Step 5 In the navigation pane on the left, choose **Authorization > Orphan Accounts** to access the orphan accounts page.

Step 6 On the orphan account page, click **add Accounts**, enter the account information.

Step 7 Click **Save**. The orphan account is added and displayed in the orphan account list. The account attributes displayed on this page can be configured based on the attribute definition of the application account. For details, see [Application Accounts](#).

----End

Enabling or Disabling an Account



Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 Click the application icon to access the general information page.

Step 5 In the navigation pane on the left, choose **Authorization > Orphan Accounts** to access the orphan accounts page.

Step 6 On the orphan accounts page, click  in the **Status** column to disable an account or click  to enable an account.

----End

Modifying an Account

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 Click the application icon to access the general information page.

Step 5 In the navigation pane on the left, choose **Authorization > Orphan Accounts** to access the orphan accounts page.

Step 6 Click **Modify** in the **Operation** column of the target orphan account to modify its information. The account attributes displayed on this page can be configured based on the attribute definition of the application account. For details, see [Application Accounts](#).

----End

Binding a User

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 Click the application icon to access the general information page.

Step 5 In the navigation pane on the left, choose **Authorization > Orphan Accounts** to access the orphan accounts page.

Step 6 In the **Operation** column of the target orphan account, choose **More > Bind to User** in the **Operation** column of the target orphan account. In the displayed dialog box, enter an existing username.

Step 7 Click **OK** to bind the orphan account to the user. If the entered user does not exist, the system displays a message indicating so.

Once bound, the orphan account is automatically moved to the application account. You can view the account in the application account list.

----End

Transferring To a Shared Account

Step 1 Log in to the administrator portal.

- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Orphan Accounts** to access the orphan accounts page.
- Step 6** In the **Operation** column of the target orphan account, choose **More > Change to Shared Account**.
- Step 7** Click **OK**. The orphan account is changed to a shared account.

Once transferred, the orphan account is automatically moved to the shared account. You can view the account in the shared account list.

----End

Deleting an Account

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Orphan Accounts** to access the orphan accounts page.
- Step 6** In the **Operation** column of the target orphan account, choose **More > Delete**.
- Step 7** Click **OK** to delete the account.

----End

4.3.2.9.5 Managing Shared Accounts

A shared account is used by multiple users. You can configure a responsible person to authorize the users to manage the account. For details, see [Shared Accounts](#).

If synchronization parameters have been configured and the synchronization is normal, adding, editing, and deleting shared accounts will trigger synchronization to downstream applications. For details, see [Synchronizing Data to Applications Through Event Callback](#).

Adding Accounts

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.



- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Shared Accounts** to access the shared accounts page.
- Step 6** Click **add Accounts** and enter the account information.
- Step 7** Click **Next**. On the displayed page, add a responsible person, and click **Save**. The added shared account is displayed in the shared account list.
- If the entered responsible person exists, after you click **Save**, the responsible person of the shared account is displayed.
 - If the entered username does not exist, the responsible person of the shared account is empty.

 **NOTE**

- If the responsible person of the shared account is empty, you can add one. For details, see [Responsible person](#).
- The account attributes displayed on the shared account adding page can be configured based on the attribute definition of the application account. For details, see [Application Accounts](#).

----End

Enabling or Disabling an Account

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Shared Accounts** to access the shared accounts page.
- Step 6** Click  in the **Status** column of the target account to disable the account or click  to enable the account.
- If a user only has permission to use a shared account, disabling the account will remove the application from the user's portal and prevent access. Enabling the account will display the application for access on the user's portal again. For details about how to access an application, see [Logging In to the User Portal and Accessing Applications](#).
 - If a user can use a shared account and also owns an application account, the application is still displayed on the user portal of the user after the shared account is disabled. When the user accesses the application, the application account information is used. After the shared account is enabled, the user can select an account for accessing the application. For details about how to access an application, see [Logging In to the User Portal and Accessing Applications](#).

----End

Modifying an Account

- Step 1** Log in to the administrator portal.
 - Step 2** On the top navigation bar, choose **Resources > Applications**.
 - Step 3** On the displayed page, click an application name to access the application details page.
 - Step 4** Click the application icon to access the general information page.
 - Step 5** In the navigation pane on the left, choose **Authorization > Shared Accounts** to access the shared accounts page.
 - Step 6** Click **Modify** in the **Operation** column of the target shared account to modify the shared account information. The account attributes displayed on this page can be configured based on the attribute definition of the application account. For details, see [Application Accounts](#).
- End

Adding a Responsible Person

- Step 1** Log in to the administrator portal.
 - Step 2** On the top navigation bar, choose **Resources > Applications**.
 - Step 3** On the displayed page, click an application name to access the application details page.
 - Step 4** Click the application icon to access the general information page.
 - Step 5** In the navigation pane on the left, choose **Authorization > Shared Accounts** to access the shared accounts page.
 - Step 6** Choose **More > Principal** in the **Operation** column of the target account. In the displayed dialog box, enter the username of the new responsible person.
 - Step 7** Click **OK** to adding a responsible person. The user can manage users through the shared account on the user portal. For details, see [Shared Accounts](#).
- End

Adding a User

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Applications**.
- Step 3** On the displayed page, click an application name to access the application details page.
- Step 4** Click the application icon to access the general information page.
- Step 5** In the navigation pane on the left, choose **Authorization > Shared Accounts** to access the shared accounts page.
- Step 6** Choose **More > Select Users** in the **Operation** column of the target account. On the displayed page, select the users to be authorized.

Step 7 Click **Save**. The user is added. After logging in to the user portal, the responsible person can manage authorized users through the shared account. For details, see [Shared Accounts](#).

----End

Deleting an Account

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 Click the application icon to access the general information page.

Step 5 In the navigation pane on the left, choose **Authorization > Shared Accounts** to access the shared accounts page.

Step 6 In the **Operation** column of the target shared account, choose **More > Delete**.

Step 7 Click **OK** to delete the account.

----End

4.3.2.10 API Permission Management

You can authorize API access to specific applications. For details, see [Authorizing Access to Built-in APIs](#).

After the authorization, APIs can be called using authorized applications. For details, see [Calling Built-in APIs](#).

4.3.2.11 Application Permission Management

You can allow OneAccess users to access applications based on their permissions through the application permissions module. After user permissions are granted, if the user needs to return the permission information to the application system, you need to configure the mapping. For details, see [Mappings](#).

You can manage application permissions only by roles or by roles, permissions, and resources.

Managing Permissions by Roles

It is a type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Users with different responsibilities are granted the corresponding roles. Roles and permissions are managed by the application.

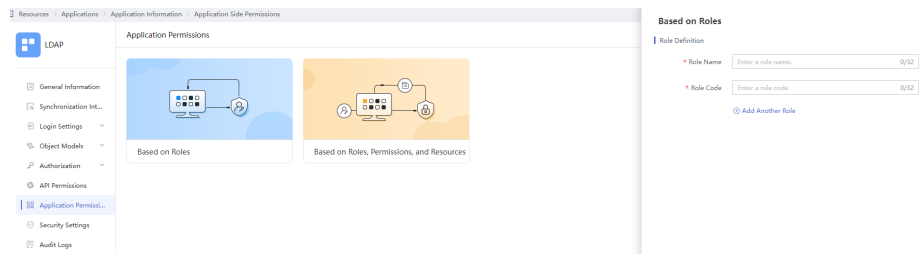
Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 In the application permission module, click **Configure**.

Step 5 Click **Based on Roles**, enter role information, you can also click **Add Another Role** to add multiple roles, and click **Save**. After you add the roles, they will be displayed in the application roles page for you to manage permissions.



----End

You can add roles, edit roles, add members, and delete roles.

- On the application roles page, click **Add Role**, enter a role name and role code, and click **OK**.
- Click **Modify** in the **Operation** column to change the role name.
- Click **Add Member** in the **Operation** column, select the accounts to which the permission is to be granted, and click **OK**. To grant multiple role permissions to an account, click to enable **Multiple Roles for Each User**. This function cannot be disabled after being enabled.
- Click **Delete** in the **Operation** column, in the displayed dialog box, click **OK**. If an application role has a referenced account, the application role cannot be deleted.

Managing Application Permissions by Roles, Permissions, and Resources

It is a fine-grained authorization mechanism that allows you to manage permissions for specific application resources based on roles. This mechanism meets the requirements for security control with the least privilege. For example, as an enterprise administrator, you can authorize users to perform specific operations on data resources of the application.

When tree-structured resource permissions are assigned to a role, the parent and child resources can be assigned independently.

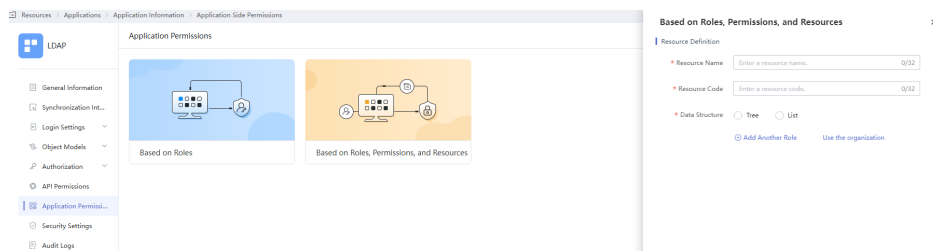
Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 In the application permission module, click **Configure**.

Step 5 On the displayed page, click **Based on Roles, Permissions, and Resources**, enter the resource name and resource code, and select the data structure. Click the add button to add more resources. You can also click **Use the organization** to call the application organization information.



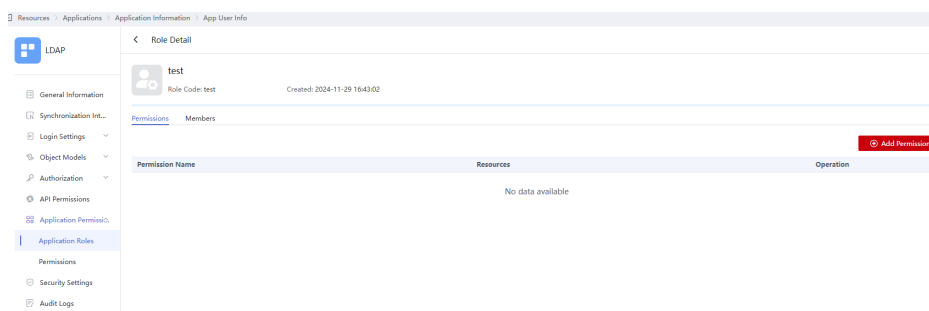
Step 6 Click **Next**. In the displayed page, enter a permission name and permission code, and select a resource and permission type. You can click the add button to add multiple permissions.

Step 7 Click **Next**, enter a role name and role code, and click the add button to add more roles. Click **Finish**. The application role and permission module are generated for you to view the added roles and permissions.

----End

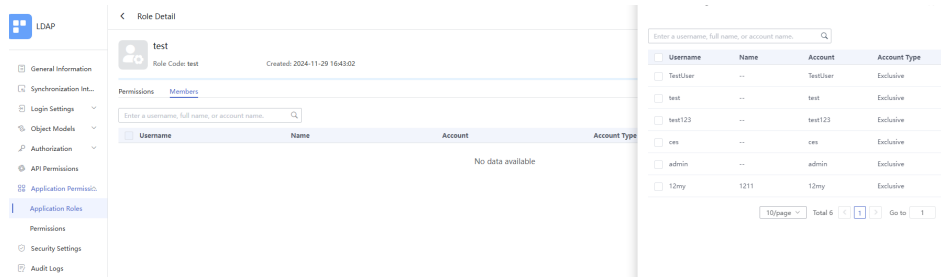
On the application roles page, you can add roles, edit roles, add permissions, add members, delete roles, and manage permissions and members.

- On the application roles page, click **Add Role**, enter a role name and role code, and click **OK**.
- Click **Modify** in the **Operation** column to change the role name.
- Click **Add Permissions** in the **Operation** column, select a permission name, select all resources or specific resources, and click **OK**.
- Click **Add Member** in the **Operation** column. Select the account to which the role permission is to be granted and click **OK**. After the member is added, you can view it in the authorized role list of the corresponding resource. To grant multiple roles to an account, click to enable **Multiple Roles for Each User**. This function cannot be disabled once enabled.
- Click **Delete** in the **Operation** column, in the displayed dialog box, click **OK**. If an application role has a referenced account, the application role cannot be deleted.
- Click the role name. On the **Permissions** tab page, click **Add Permission** to grant permissions to the role.

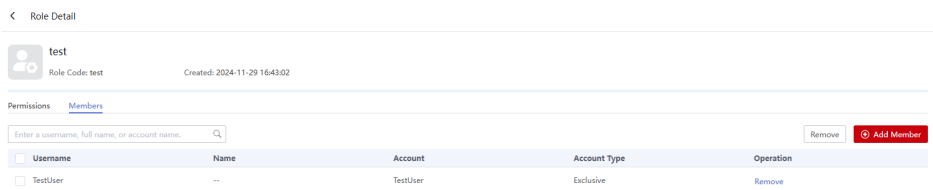


- On the **Permissions** tab page, click **Modify** in the **Operation** column to modify a permission.
- On the **Permissions** tab page, click **Cancel Authorization** in the **Operation** column to cancel the authorization.
- Click the role name and go to the **Members** tab page.

- Click **Add Member** to add members to the role.



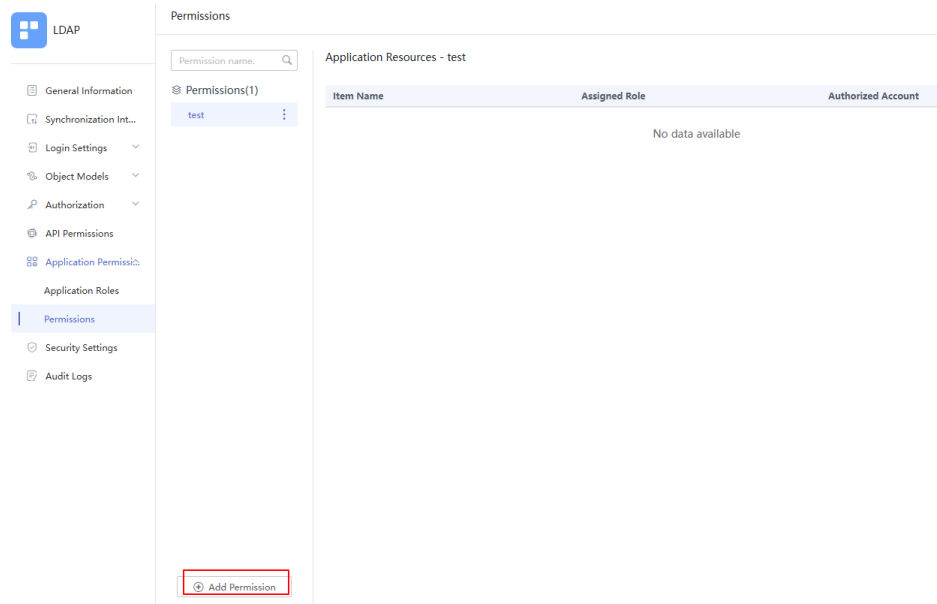
- On the member management page, select the members to be removed and click **Remove** in the upper right part. You can also click **Remove** in the **Operation** column to remove specific members.




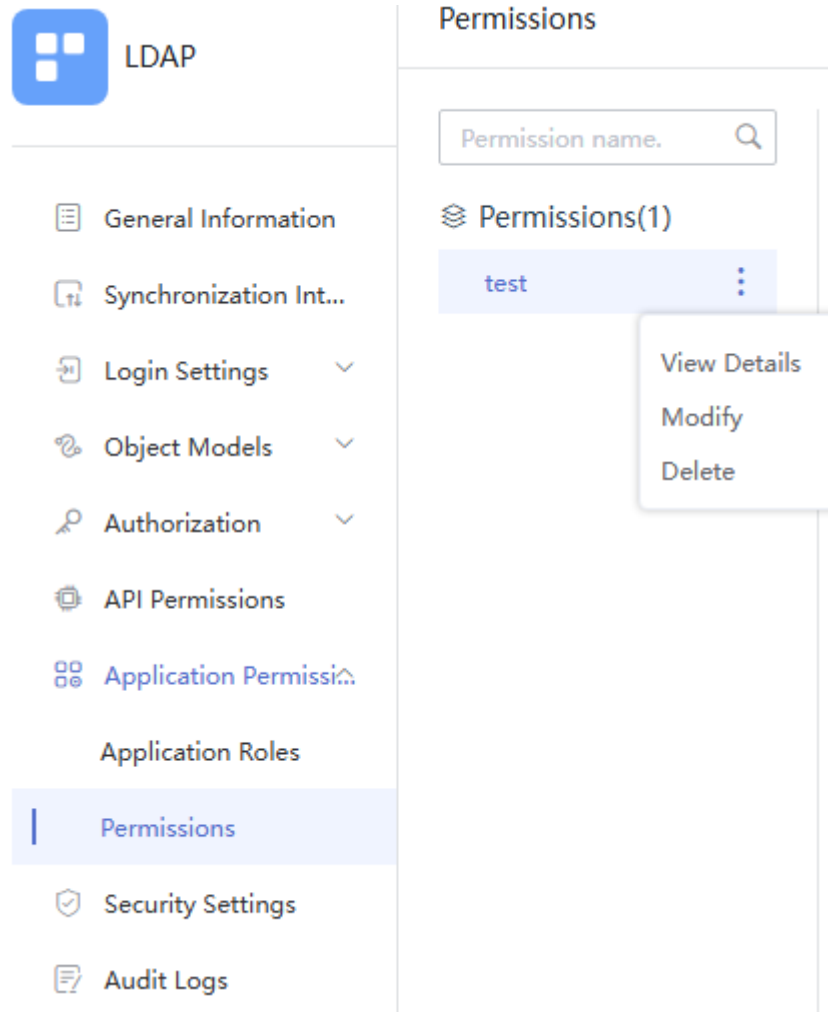
You can manage permissions and resources.



- Permissions

- On the permission page, click **Add Permission** to add a permission. The permission code must be unique.



- Click  on the right of the permission name and click **View Details** to view the permission details, including the permission name, code, and resources.



- Click  on the right of the permission name and click **Modify** to modify the permission name and type.
- Click  on the right of the permission name and click **Delete** to delete the permission.
- Resources

Application organizations can be regarded as resources. For details about how to maintain application organizations, see [Managing Application Organizations](#). Before using the application organization, you need to enable it. For details, see [Application Organizations](#). There is tree and list data structure. You can create a multi-level structure if you select the tree data structure. By default, an application organization uses the tree data structure. An item is a subset of a resource. Operations on resources are also applicable to items. The operations include adding, modifying, and deleting. The following uses resources as an example.

 - a. On the permissions page, click **Manage Resources**. The application resource page is displayed.
 - b. Click **Add Resource**, enter a resource name and code, and select a data structure.
 - c. Click **OK**. The resource is added successfully and is displayed in the resource list.

You can manage resources by adding items, editing resources, and deleting resources.

- Click **Add Item** in the **Operation** column to add an item to the resource. If the resource uses the tree data structure, you can add sub-items to the item. Items belonging to a resource have unique codes.
- Click **Modify** in the **Operation** column to modify the resource. To modify an item, click **Modify** in the **Operation** column. Click **Modify** for an application organization, the application organization page is displayed. For details about how to maintain an application organization, see [Managing Application Organizations](#).
- Click **Delete** in the **Operation** column of a resource to delete the resource. To delete an item, click **Delete** in the **Operation** column of the item.

4.3.2.12 Security Settings

You can configure the egress IP address of the server for calling open APIs. If the egress IP address is not configured, open APIs can be called. The last digit of the IP address can be a wildcard character (*). A maximum of 10 IP addresses separated by commas (,) are allowed. For example, **192.168.0.*,192.168.1.1**.

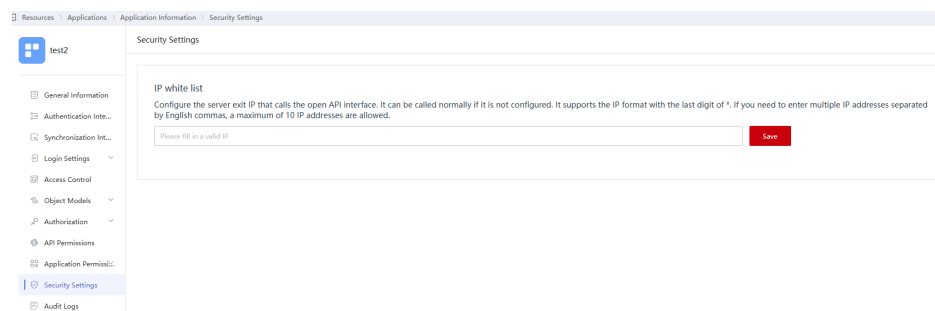
Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 Click the application icon to access the general information page.

Step 5 Select **Security Settings**.



Step 6 Enter a valid IP address in the text box and click **Save**.

----End

4.3.2.13 Audit Logs

You can check the operation records of the administrator on an application. In addition, you can filter the operation records by start time, end time, and administrator.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Applications**.

Step 3 On the displayed page, click an application name to access the application details page.

Step 4 Click the application icon to access the general information page.

Step 5 Click **Audit Logs** to check the operation records of the administrator on the application.

Time	Operator	Operation Type	Client IP Address	Location	Batch operation	Result	Operation
2022-08-23 15:48:14	12my	Application organization ...	192.168.1.72	local area network	No	--	Details
2022-08-23 15:48:14	12my	Save organization author...	192.168.1.72	local area network	No	--	Details
2022-08-23 15:36:04	12my	Delete application account	192.168.1.72	local area network	No	--	Details
2022-08-23 15:36:01	12my	Delete application account	192.168.1.72	local area network	No	--	Details
2022-08-23 15:35:52	12my	Application organization ...	192.168.1.72	local area network	No	--	Details
2022-08-23 15:35:51	12my	Save organization author...	192.168.1.72	local area network	No	--	Details
2022-08-23 15:35:36	12my	Delete virtual organization	192.168.1.72	local area network	No	--	Details
2022-06-17 15:21:51	12my	Add shared account	192.168.1.72	local area network	No	--	Details
2022-06-17 15:14:19	12my	Change controller	192.168.1.72	local area network	No	--	Details
2022-06-17 15:13:58	12my	Change controller	192.168.1.72	local area network	No	--	Details

----End

4.3.3 APIs

4.3.3.1 Authorizing Access to Built-in APIs

You can authorize API access to specific applications.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Enterprise APIs**.

Step 3 On the displayed page, choose **System APIs > Built-in APIs**, click the **Application Authorization** tab, and click **Authorize** in the row that contains the target application to authorize it to access the built-in APIs.

Step 4 Go to the application details page, and authorize the application to access specific APIs. For details about how to add an application, see [Integrating Enterprise Applications](#).

NOTE

To authorize an application to call **auth_api** for account binding, registration, or both, ensure that you have set the authentication method of the application to **OPEN_API**.

1. On the top navigation bar, choose **Resources > Applications**.
2. Click the name of the application authorized in [Step 3](#).
3. Click the application icon to access the general information page.
4. Choose **API Permissions > Built-in APIs**. On the displayed page, click **Authorize** in the **Operation** column of a permission code. The following table lists the mapping between permissions and APIs.

Table 4-19 Mapping between permissions and APIs

Per mission Code	Per mission Description	API Description	API URL	Remarks
user_all	Read and write permissions for user management APIs	Creating a user	POST /api/v2/tenant/users	-
		Modifying a user	PUT /api/v2/tenant/users/{user_id}	-
		Deleting a user	DELETE /api/v2/tenant/users/{user_id}	-
		Disabling a user	PUT /v2/tenant/users/{user_id}/disable	-
		Enabling a user	PUT /v2/tenant/users/{user_id}/enable	-
		Changing the password	PUT /api/v2/tenant/users/{user_id}/change-password	-
		Verifying the original password and changing the user password	PUT /api/v2/tenant/users/{user_id}/change-password-verify	-
		Authorizing an application account	POST /api/v2/tenant/users/{user_id}/applications/{application_id}/accounts	-
		Querying user details by user ID.	GET /api/v2/tenant/users/{user_id}	user_read permission
		Obtaining all application accounts of a user	GET /api/v2/tenant/users/{user_id}/accounts	user_read permission
Querying users	GET /api/v2/tenant/users	user_read permission		

Per mission Code	Per mission Description	API Description	API URL	Remarks
org_all	Read and write permissions for organization management APIs	Creating an organization	POST /api/v2/tenant/organizations	-
		Modifying an organization	PUT /api/v2/tenant/organizations/{org_id}	-
		Deleting an organization	DELETE /api/v2/tenant/organizations/{org_id}	-
		Querying organization details	GET /v2/tenant/organizations/{org_id}	org_read permission
		Querying organizations	GET /api/v2/tenant/organizations	org_read permission
account_all	Read and write permissions for application account management APIs	Creating an application account	POST /api/v2/tenant/applications/{application_id}/accounts/basic-account	-
		Updating an application account	PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}	-
		Deleting an application account	DELETE /api/v2/tenant/applications/{application_id}/accounts/{account_id}	-
		Querying application accounts	GET /v2/tenant/applications/{application_id}/accounts	account_read permission
		Querying application accounts	GET /api/v2/tenant/applications/{application_id}/accounts/{account_id}	account_read permission

Per miss ion Cod e	Per miss ion Des crip tion	API Descriptio n	API URL	Remar ks
		Disabling an application account	PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}/disable	-
		Enabling an application account	PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}/enable	-
app_ org_ all	Rea d and writ e per miss ions for appl icati on orga niza tion man age men t APIs	Querying authorized application organizations	GET /api/v2/tenant/applications/{application_id}/organizations	app_or g_read permiss ion
		Querying application organization details	GET /api/v2/tenant/applications/{application_id}/organizations/{org_id}	app_or g_read permiss ion
		Adding an application organization	POST /api/v2/tenant/applications/{application_id}/organizations	-
		Modifying an application organization	PUT /api/v2/tenant/applications/{application_id}/organizations/{org_id}	-
		Deleting an application organization	DELETE /api/v2/tenant/applications/{application_id}/organizations/{org_id}	-

Per miss ion Cod e	Per miss ion Des crip tion	API Descriptio n	API URL	Remar ks
app_rol e_ all	Rea d and writ e per miss ions for appl icati on role APIs	Adding an application role	POST /api/v2/tenant/applications/{application_id}/role	-
		Modifying an application role	PUT /api/v2/tenant/applications/{application_id}/role/{role_id}	-
		Deleting an application role	DELETE /api/v2/tenant/applications/{application_id}/role/{role_id}	-
		Adding an application role member	POST /api/v2/tenant/applications/{application_id}/role-member	-
		Deleting an application role member	DELETE /api/v2/tenant/applications/{application_id}/role-member	-
		Querying application roles	GET /api/v2/tenant/applications/{application_id}/role-list	app_rol e_read
		Querying application role details	GET /api/v2/tenant/applications/{application_id}/role/{role_id}	app_rol e_read
		Querying application role members	GET /api/v2/tenant/applications/{application_id}/role-member-list/{role_id}	app_rol e_read
all	Rea d and writ e per miss ions for all OAP APIs	All preceding APIs	-	-

----End

4.3.3.2 Calling Built-in APIs

You can call APIs using authorized applications.

- Step 1** Log in to the administrator portal.
- Step 2** In the top navigation pane, choose **Resources > Enterprise APIs**, click the API to be called.
- Step 3** On the **Application Authorization** tab page, click **Authorize** in the **Operation** column to authorize the specified application to call the built-in API.
- Step 4** On the top navigation bar, choose **Resources > Applications**, click an application name.
- Step 5** On the displayed application information page, obtain client ID and client secret of the application.
- Step 6** Click the application name to access the general information page.
- Step 7** Select **API Permissions**. On the displayed page, authorize the required API permissions to the application by referring to [Step 4](#).
- Step 8** Obtain access token based on the values of client ID and client secret obtained in [6](#). For details, see [Obtaining Access Credentials](#).
- Step 9** Call the built-in APIs of OneAccess using the authorized access token.

----End

4.3.3.3 Modifying Built-in APIs

Modify the permission codes and descriptions of built-in APIs. The basic information cannot be modified.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Resources > Enterprise APIs**.
- Step 3** On the displayed page, choose **System APIs > Built-in APIs** to go to the enterprise API details page.
- Step 4** Switch to the **Application Authorization** tab page and modify application authorization. Click **Authorize** or **Cancel Authorization** in the **Operation** column of an application to authorize or cancel the authorization of the application to call the built-in APIs. For details about how to add an application, see [Integrating Enterprise Applications](#).
- Step 5** Click the **Permissions** tab to modify permissions. Click **Modify** in the **Operation** column of the row that contains the target permission, modify the permission description, and determine whether to set the permission as the default.

Table 4-20 Permission parameters

Parameter	Description
* Permission Code	Only letters and underscores (_) are allowed.
Description	Description of the permission.
Default Permission	Deselected by default. <ul style="list-style-type: none">• If you select this option, authorized applications have this permission by default, and you do not need to grant the permission again.• To remove a default permission of an application, change the default permission to a non-default one and then cancel the authorization.

Step 6 Switch to the **Audit Logs** tab page to view audit logs. You can view the operation records of the APIs.

----End

4.3.3.4 Adding a Custom API

Add custom APIs in the administrator portal and authorize access to specific applications.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Enterprise APIs**.

Step 3 On the displayed page, click **Add Custom APIs**.

Step 4 Upload a logo, enter the product name and description, and click **OK**.

----End

4.3.3.5 Configuring a Custom API

APIs can be called only by applications that have been granted access to them. You can customize API to add the built-in API permission code to grant the API permission to the target application. In addition, you can customize API to add the external API permission.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Enterprise APIs**.

Step 3 On the **Enterprise APIs** page, click the target custom API.

Step 4 On the **Basic Information** tab page, modify the product logo, name, and description.

Step 5 Switch to the Application Authorization tab page and modify the application permission to call the API. For details about how to add an application, see [Adding an Application](#).

 **NOTE**

After you grant API access to an application, go to the application details page, and authorize the application to access the API. For details, see [Step 4](#).

Step 6 Switch to the **Permissions** tab page and click **Add** to add a permission code. (The permission code can be a built-in API or external API.)


Step 7 Switch to the **Audit Logs** tab page to view audit logs. You can view the operation records of the APIs.

----End

4.3.3.6 Deleting a Custom API

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Resources > Enterprise APIs**.

Step 3 On the displayed page, click  in the upper right corner of the target custom API product, and click **Delete**. In the displayed dialog box, click **OK**.

 **NOTE**

If you delete an enterprise API, applications that have been granted access to it can no longer call the API. Exercise caution when performing this operation.

----End

4.4 Authentication

4.4.1 Managing Authentication Providers

OneAccess supports authentication with both individual and enterprise (internal and external) authentication providers, providing a good login experience for users in your enterprise. As an administrator, you can add, modify, and delete authentication providers.

 **NOTE**

You can use both local and third-party authentication providers, and you are advised to select a secure authentication method.

This section uses WeLink as an example to describe how to configure an individual social authentication provider. For details about how to configure other authentication providers, see [Authentication Provider Integration](#).

Adding an Authentication Provider

 **NOTE**

- Ensure that you have administrator permissions for the WeLink open platform.
- Ensure that you have created an application on the WeLink open platform.

Step 1 Log in to the administrator portal.

- Step 2** On the top navigation bar, choose **Authentication > Authentication Providers**.
- Step 3** On the **Authentication Providers** page, choose **Enterprise Social Authentication > WeLink**.
- Step 4** Set the WeLink application parameters.

Table 4-21 Parameter description

Parameter	Description
Display Name	Name of the authentication provider.
AppKey	Client ID of an application that you have created on the WeLink open platform.
AppSecret	Client secret of the application.
Source Attribute	User attribute configured for the application. mobileNumber , userNameCn , userNameEn , userEmail , and corpUserId are supported.
Related User Attribute	OneAccess user attribute to which the user attribute of the WeLink application will be mapped. Choose any attribute from the mobile number, user ID, username, and email address.
No User Associated	Select an operation that will be performed if a user is not mapped to any system user during login. The options include Bind , Bind or Register , Automatically create users , and Failed .

- Step 5** Click **Save**.
- End

Modifying an Authentication Provider

Modify the settings of an authentication provider.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Authentication > Authentication Providers**.
- Step 3** On the **Authentication Providers** page, choose **Enterprise Social Authentication > WeLink**.
- Step 4** Modify the WeLink application parameters.
- Step 5** Click **Save**.
- End

Deleting an Authentication Provider

 NOTE

- If an authentication provider is deleted, all data of the authentication provider will also be deleted and cannot be recovered.
- Enterprise social authentication providers can be disabled but cannot be deleted.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Authentication > Authentication Providers**.

Step 3 On the **Authentication Providers** page, click the target authentication provider.

Step 4 Click **Delete** in the **Operation** column of an authentication provider.

Step 5 In the displayed dialog box, click **OK**.

----End

4.4.2 Managing Regions

Use regions to allow or deny access of specific users to specific applications.

Adding a Region

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Authentication > Regions**.

Step 3 On the **Regions** page, click **Add Region**.

Step 4 Enter the region information.

Table 4-22 Region information

Parameter	Description
* Region Name	Name of a logical area in your enterprise. For example, a development region.
* IPv4 CIDR Block	IPv4 CIDR block of the region. The value must be unique.
Description	Description about the region.

Step 5 Click **Save**.

----End

Modifying a Region

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Authentication > Regions**.

Step 3 In the region list, click **Modify** On the **Operation** column of the target region, and modify the parameters described in [Table 4-22](#).

Step 4 Click **Save**.

----End

Deleting a Region

NOTE

Deleted regions cannot be recovered.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Authentication > Regions**.

Step 3 In the region list, click **Delete** On the **Operation** column of the target region.

Step 4 In the displayed dialog box, click **OK**.

----End

4.4.3 Managing Authentication Strategies

OneAccess simplifies user access management by offering a unified solution. With authentication strategies, you can control access for specific users based on factors like access time, device type, and region range. Furthermore, you can allow access, deny access, or enable multi-factor authentication (MFA) for specified users.

Adding an Authentication Strategy

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Authentication > Authentication Strategy**.

Step 3 On the displayed page, click **Add a strategy**.

Step 4 Configure the strategy.

Table 4-23 Strategy parameters

Parameter	Description
*Policy Name	Name the added authentication strategy for easy management.
Description	Add a description for the authentication strategy.
User Condition	Select the user range. The options include All users , Qualified users , and Disqualified users .
Access Time	Time range when users are allowed or not allowed to access the application. The options include Any time , Within specific periods , and Outside specific periods .
Device Type	Type of devices that are allowed or not allowed to access the application. The options include Browser , Desktop device , and Mobile device .

Parameter	Description
Regions	Set the region range. The options include Any, Chinese Mainland, Outside the Chinese Mainland, Within specific regions, Outside specific regions.
Authentication Provider	Select authentication provider that users can or cannot use to access the application. The options include Any, With specific authentication providers, and Without specific authentication providers.
Risk operation	Select the user who triggers a risk event. You can select multiple users, which is the same as the risk event in risk behavior management.
Access control	Specify how to manage user access. You can choose to allow access, deny access, or enable multi-factor authentication (MFA) for users who meet specific criteria. NOTE If MFA authentication is selected, five authentication modes are available: OTP, SMS, email, FIDO2, and fingerprint authentication.

Step 5 Click **Save**.

----End

Modifying an Authentication Strategy

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Authentication > Authentication Strategy**.

Step 3 On the authentication strategy page, click **Modify** in the **Operation** column of the target strategy. On the displayed page, modify the authentication strategy configuration.

Step 4 Click **Save**.

----End

Deleting an Authentication Strategy

You can delete authentication strategies as needed.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Authentication > Authentication Strategy**.


Step 3 Click **Delete** in the **Operation** column of the target strategy.

Step 4 Click **OK**.

----End


Disabling an Authentication Strategy

If you do not want to use the authentication strategy in a certain period, you can disable it by changing its status.

- Step 1** Log in to the administrator portal.
 - Step 2** On the top navigation bar, choose **Authentication > Authentication Strategy**.
 - Step 3** In the **Status** column of the target strategy, click .
 - Step 4** In the displayed dialog box, click **OK** to disable the strategy.
- End

Enabling an Authentication Strategy

If an authentication strategy has been disabled, you can enable it when you need to use it.

- Step 1** Log in to the administrator portal.
 - Step 2** On the top navigation bar, choose **Authentication > Authentication Strategy**.
 - Step 3** In the **Status** column of the target strategy, click .
 - Step 4** In the displayed dialog box, click **OK** to enable the strategy.
- End

Adjusting the Strategy Priority

A maximum of 10 authentication strategies can be added. You can drag a strategy in the authentication strategy list to change its priority.

- Step 1** Log in to the administrator portal.
 - Step 2** On the top navigation bar, choose **Authentication > Authentication Strategy**.
 - Step 3** Drag the target strategy upwards or downwards to a desired sequence.
- End

4.5 Security

4.5.1 Managing Administrator Permissions

You can add administrators and administrator groups and grant them specific permissions for the administrator portal.

There are super administrators, common administrators, and system administrators.

- Super administrators have permissions to manage all organizations, applications, and menus in the administrator portal.

- Common administrators have permissions to manage only specific organizations, applications, and menus (except the menus on the homepage) in the administrator portal.
- System administrators have permissions to manage all organizations, applications, and menus (except those in the administrator permission function) in the administrator portal. They are accounts generated by tenant sub-accounts logging in to the administrator portal.

 **NOTE**

System administrators are in the system management group by default, which is not displayed in the administrator portal.

Adding a Super Administrator

Use a tenant account to log in to the administrator portal, add an administrator to the super management group to grant it full permissions for the administrator portal.


- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Security > Administrator Permissions**.
- Step 3** On the **Administrators** tab page, click  **Add Administrator**.
- Step 4** Enter the administrator information.

Table 4-24 Administrator information

Parameter	Description
Username	Username of the administrator. It must start with a letter.
Full Name	Full name of the administrator.
Phone Number	Mobile number of the administrator. It must be different from those of other administrators.
Email Address	Email address of the administrator. It must be different from those of other administrators.
Password	Password of the administrator.
Confirm Password	Enter the password again.
Administrator Permissions	The options are Administrator Groups and Custom . By default, Administrator Groups is selected.
Administrator Groups	Select an existing administrator group to obtain the permissions of this administrator group. The super administrator group is selected by default.

Step 5 Click **Save**.

----End

Adding a Common Administrator

Log in to the administrator portal as an administrator with the administrator permissions, add an administrator, and grant permissions (not beyond those possessed by the granter) to the administrator. If the added administrator is not a super administrator, the administrator is a common administrator.


- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Security > Administrator Permissions**.
- Step 3** On the **Administrators** tab page, click  **Add Administrator**.
- Step 4** Enter the administrator information.

Table 4-25 Administrator information

Parameter	Description
Username	Username of the administrator. It must start with a letter.
Full Name	Full name of the administrator.
Phone Number	Mobile number of the administrator. It must be different from those of other administrators.
Email Address	Email address of the administrator. It must be different from those of other administrators.
Password	Password of the administrator.
Confirm Password	Enter the password again.

- Step 5** Grant permissions to the administrator.
- If **Administrator Groups** is selected, select the administrator group to which the administrator belongs from the drop-down list. The administrator inherits all permissions of the administrator group. If you do not select the default super administrator group, you can customize the permissions of the administrator group. For details about how to add an administrator group, see [Adding an Administrator Group](#).
 - If **Custom** is selected, the common administrator does not belong to any administrator group. You can customize permissions for the common administrator by selecting all or specific organizations, applications, and menus (except the menus on the homepage).

The screenshot shows the 'Add Administrator' form in the OneAccess Administrator Permissions interface. The form is divided into two main sections: 'Super Administrators' and 'Common Administrators'. The 'Super Administrators' section shows a list of administrators, with '12 Creator' selected. The 'Common Administrators' section shows 'No Data'. The 'Custom' section also shows 'No Data'. Below these sections is a '+ Add Administrator' button. The 'Add Administrator' form itself includes the following fields and options:

- * Username: admin
- * Full Name: sss
- * Phone Number: +86 (country code dropdown) and a masked phone number field.
- * Email Address: masked email field.
- * Password: masked password field.
- * Confirm Password: masked confirm password field.
- * Administrator: Radio buttons for 'Administrator Groups' and 'Custom' (selected).
- Permissions: Checkboxes for 'Organizations', 'Applications', and 'Menus', each with 'All' (selected) and 'Specific' options.
- Buttons: 'Cancel' and 'Save' (highlighted in red).

Step 6 Click **Save**.

----End

Modifying Administrator Information

On the **Administrators** tab page, click the name of the target administrator, click **Modify**, modify the basic information, and change the administrator group.

NOTE

- To modify the information about the enterprise account creator, see [Setting the Tenant Type](#).
- If you add a super administrator to a common administrator group or grant the administrator only specific permissions, the super administrator becomes a common administrator.

Changing the Password of an Administrator

On the **Administrators** tab page, click the name of the target administrator, click **Change Password**, enter the new password, and click **Save**.

NOTE

The creator of the super administrator and the system administrator cannot change the password.

Deleting an Administrator

On the **Administrators** tab page, click the name of the target administrator, click **Delete**, and then click **OK**.

 NOTE

Deleted administrators can no longer access the administrator portal. For details about how to add an administrator, see [Adding a Super Administrator](#) or [Adding a Common Administrator](#).

Adding an Administrator Group

Add an administrator group and grant it specific permissions for the administrator portal.

 NOTE

Menus on the homepage are unavailable when you grant menu permissions to a sub-administrator group.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Administrator Permissions**.

Step 3 Click the **Administrator Groups** tab.

Step 4 Click the administrator group under which you want to add a new administrator group, and click **Add**.

Step 5 On the **Add Administrator Group** page, enter the administrator group name, grant permissions for all or specific organizations, applications, and menus of the administrator portal, and click **Save**.

----End

Modifying Administrator Group Information

 NOTE

If you modify the permissions of an administrator group, permissions of the administrators in the group will also change.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Administrator Permissions**.

Step 3 Click the **Administrator Groups** tab.

Step 4 On the administrator page, click the target group.

Step 5 On the right part of the displayed page, click **Modify**. You can modify the name and permissions of the administrator group.

Step 6 Click **Save**.

----End

Deleting an Administrator Group

Before you delete an administrator group, ensure that the group has no members.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Administrator Permissions**.

Step 3 Click the **Administrator Groups** tab.

Step 4 On the administrator page, click the target group.

Step 5 On the right part of the displayed page, click **Delete**.

Step 6 In the displayed dialog box, click **OK**.

----End

4.5.2 Managing Password Policies

The password policy consists of password strength, login security, advanced settings, and password initialization settings.

NOTE

- Configure the password policy to ensure that users use strong passwords.
- The password policy takes effect for all users created in the OneAccess instance.

Password Strength

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Password Policy**.

Step 3 Click the password strength area. Configure the password length, complexity, and restrict consecutive identical characters, and detect weak password or password containing user information.

- Password length

Set the minimum and maximum password lengths. By default, a password must contain 8 to 18 characters. The minimum and maximum password lengths range from 8 to 50 characters.

- Password complexity

Set the types of characters that a password must contain. For example, a password must contain at least three types of the following: digits, uppercase letters, lowercase letters, and special characters.

NOTE

The following special characters are supported: ~!#\$%&+,-;*;<=>@_?^`./

- Restrict consecutive identical characters

Configure whether to allow consecutive identical characters in a password and how many such characters are allowed. By default, a password cannot contain consecutive identical characters. If you enable this option, set the maximum of consecutive identical characters allowed from 1 to 10. Value **1** indicates that consecutive identical characters are not allowed in a password.

- Restrict user information

Configure whether to allow user information in a password. By default, this option is disabled. If you enable this option, the password of a user cannot contain the username, mobile number, or email prefix of the user.

- Weak password check
Configure whether to check weak passwords. If you enable this option, passwords included in the weak password list are not allowed.

Step 4 Click **Save**.

----End

Login Security

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Password Policy**.

Step 3 Click the login security area. Configure the time and conditions for locking an account.

- Account lockout

Set the number of unsuccessful login attempts to lock users out if the number is reached during login. The value ranges from 1 to 10, and the default value is 10.

NOTE

If the number of login failures exceeds the threshold, the sliding verification code is enabled. The threshold is automatically calculated as one-third of the number for locking an account.

- Account unlock

Set a duration to unlock users after users are locked out. The value ranges from 1 to 1440 minutes, and the default value is 3 minutes.

Step 4 Click **Save**.

----End

Advanced Settings

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Password Policy**.

Step 3 Click the advanced settings area. Configure whether to check username spelled backwards, previously used passwords, and password expiration.

- Check for username spelled backwards

Configure whether the password of a user can be the username spelled backwards. By default, this option is disabled. If you enable this option, the password of a user cannot be the username spelled backwards.

- Check for previously used passwords

Configure whether to allow a password to be a historical password. By default, this option is disabled. If you enable this option, the password of a user cannot be one of the specified number of historical passwords. The value ranges from 1 to 10, and the default value is 5. For example, value **3** indicates that a user cannot set the last three passwords that the user has previously used, when the user sets the new password.

- Password expiration
Configure whether to prompt users to change their passwords when the passwords are about to expire. By default, this option is disabled. If you enable this option, users will be prompted to change their passwords when the passwords will expire in a specific number of days. After the passwords expire, users will be required to change their passwords when they log in to the user portal. The default password validity period is 120 days. Set a validity period greater than or equal to 1 day. The default number of days for prompting password change is 5 days. Set a number greater than or equal to 1 and less than or equal to the password validity period.

 **NOTE**

The password expiration setting keeps user accounts secure.

Step 4 Click **Save**.

----End

Password Initialization Settings

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Password Policy**.

Step 3 Click the password initialization settings area. Configure whether to enable the password initialization, notification mode, and validity period.

- Enabling password initialization
To enable this function, you need to add valid contact information of the user. Otherwise, the user cannot be notified. After the function is enabled, you can choose to automatically generate a password.
- Notification mode
Notifications can be sent by email or SMS message. For email notifications, you need to configure the email gateway first by referring to [Email Gateway](#). If both email and SMS are selected, the system preferentially sends notifications to users by email.
- Validity period of the initialized password
A maximum of seven days can be set.

Step 4 Click **Save**.

----End

4.5.3 Managing Risky Behaviors

OneAccess can detect abnormal account behavior. After the function is enabled, the system detects abnormal user behavior based on the preset behavior rules. When a risk is triggered, the system sends an alarm in real time.

There are four types of risks:

- Abnormal IP address: The login IP address of the account is inconsistent with the common IP address.
- Abnormal location: The login location of an account is inconsistent with the common location.

- Abnormal device: The login device (browser or terminal device) is inconsistent with the common device.
- Account lockout: The number of incorrect password attempts exceeds the threshold set in the password policy, the account will be locked.

When the configured behavior triggers a risk, the system sends a risk notification through email, SMS, or DingTalk.

Adding a Behavior

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Risk Behavior Manage**.

Step 3 On the risky behavior management page, click **Add operation**, and set parameters.

Table 4-26 Behavior parameters

Parameter	Description
* Behavior name	Name of a risky behavior.
* Risk type	Risk event type. The options include Error location , Error device , Error IP , and Account Locked .
Location type	Abnormal location range. You can define abnormal location events based on the selected location type. NOTE This parameter is available only when location type is set to Error location .
* Frequency settings	Set a default value for the IP addresses, devices, and locations that are frequently used for login. If the default values are not used, abnormal behaviors are displayed in the risk events and risk dashboard. NOTE When risk type is set to Account Locked , this parameter is not available. If the number of incorrect password attempts exceeds the threshold specified in the password policy, the account is locked, the behavior is marked as a risk event, and is displayed in the risk events and risk dashboard.
Description	Description of the added behavior.

Step 4 Click **OK**. The behavior is added. The added risky behavior is displayed in the risky behavior list. You can filter the risky behavior by risk type.

----End

Editing a Behavior

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Risk Behavior Manage**.

Step 3 Click **Modify** in the **Operation** column of the target behavior to modify its configuration.

Step 4 Click **OK**.

----End

Deleting a Behavior

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Risk Behavior Manage**.

Step 3 Click **Delete** in the **Operation** column of the target behavior.


Step 4 Click **OK**.

----End

Disabling a Risky Behavior

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Risk Behavior Manage**.

Step 3 In the **Status** column of the target behavior, click .

Step 4 Click **OK**.


----End

Enabling a Risky Behavior

After a risky behavior is enabled, the system detects abnormal user behavior based on the preset behavior rules. When a risk is triggered, the system sends an alarm in real time.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Security > Risk Behavior Manage**.

Step 3 In the **Status** column of the target behavior, click .

Step 4 Click **OK**.

----End

Setting Notifications

When the configured behavior triggers a risk, the system sends a risk notification based on your setting.

Step 1 On the risky behavior management page, click **Notify setting**.

Step 2 In the displayed dialog box, set the notification method and objective.

Table 4-27 Notification parameters

Parameter	Description
* Notification method	Way in which the system sends a notification when a risk behavior is triggered. Notifications can be sent through email, SMS, or DingTalk. If you select email or DingTalk, set the gateway by referring to Email Gateway and DingTalk Gateway .
* Send objective	Object to which the system sends a notification when a risk behavior is triggered. By default, notifications are sent to all users. You can also exclude specified users.

Step 3 Click **OK**.

----End

4.6 Audit

OneAccess allows you to view user and administrator operation logs, risk events, and risk dashboard. It supports security analysis, audit, resource tracing, and fault locating.

Viewing User Operation Logs

You can view the operations performed by all users in the user center, including the time, name, username, operation type, and results.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Audit > User Operations**.

Step 3 Click **Details** in the **Operation** column of the target operation.

Step 4 Click **Export** in the upper right of the user operations page to export all logs.

----End

To view logs generated two years ago, click **Log Archives** in the upper right of the **User Operations** page, and click **Download** in the **Operation** column of the target log file. Decompress the package and view the time, username, operation results, and operation type in each log.

Viewing Administrator Operation Logs

You can view the operations performed by all administrators in the administrator portal, including the time, operator, operation object, and operation type.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Audit > Administrator Operations** and view administrator operation logs.

Step 3 Click **Export** in the upper right of the administrator operations page to export all logs.

----End

To view logs generated two years ago, click **Log Archives** in the upper right of the **Administrator Operations** page, and click **Download** in the **Operation** column of the target log file. Decompress the package and view the time, operation object, operation type, and location in each log.

Risky Events

You can view the risky events triggered by all users and administrators, including the trigger time, risk type, login mode, name, and username.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Audit > Risk Event**.

Step 3 You can filter risky events by start time, risk type, name, or username.

Step 4 Click **View** in the **Operation** column of the target event to check its details.

----End

Risk Dashboard

The risk dashboard displays all risk operations of an instance from a global perspective. It includes several modules. You can filter risks by time (today, last 7 days, last 30 days) or customizing a time range in the upper right part of the risk dashboard page.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Audit > Risk Dashboard** to check triggered risk behaviors.

Table 4-28 Risk dashboard

Module	Description
Number of risks today	Number of risk events triggered on the current day. The selected time period does not affect this module's statistics.
Total number of risk events	Total number of risk event logs within the selected time period.
Total number of risky users	Number of users who trigger risk events within the selected time period.
Number of risky users today	Number of users who trigger risk events on the current day. The selected time period does not affect this module's statistics.
Triggered risk type	Number of risk events of various types within the selected time period.

Module	Description
Risky user list	List of users who trigger recent risk events. Click More go to the risk event page.
Risk event list	List of recent risk events. Click More go to the risk event page.
Login risk times	<p>Number of risk events in each time range within the selected time period. Risk events statistics are displayed based on different time periods.</p> <ul style="list-style-type: none"> • Today: Statistics are collected by hour. The horizontal coordinate displays time from 00:00 to 23:00. For example, the risk event at 00:15 is collected in 00:00, the risk event at 9:30 is collected in 09:00, and the risk event at 23:45 is collected in 23:00. • Last 7 days: Statistics are collected by day. The horizontal coordinate displays the dates from 7 days ago to today. • Last 30 days: Statistics are collected by day. The horizontal coordinate displays the dates from 30 days ago to today. For example, on December 28, the number of risk events from November 29 to December 28 is displayed. • Customized time period: Statistics are collected by day. The horizontal coordinate displays the dates from the defined start date to end date.
Recent 10 detected abnormal devices	Top 10 devices with the most risk events within the specified time period. Devices are classified by device type and browser.
Top 10 detected abnormal IP addresses	Top 10 IP addresses with the most risk events within the specified time period.

----End

4.7 Settings

4.7.1 Modifying Enterprise Information

Complete your enterprise information, including industry, staff size, contact, phone number, and address, so that we can provide you services that meet your requirements.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Enterprise Information**.

Step 3 On the **Enterprise Information** page, click **Modify**, modify the basic and contact information, and click **Save**.

----End

4.7.2 Enterprise Settings

4.7.2.1 Overview

OneAccess provides multiple authentication methods to meet security requirements.

To maintain a consistent username format, you can enable the username rule. For enhanced account security, enable MFA and WeLink authentication in the administrator portal. To prevent identity spoofing or theft during login authentication, registration, password retrieval, and two-factor VPN authentication, you and other administrator can configure the user agreement, SMS gateway, voice gateway, email gateway, and DingTalk gateway to verify user identities through SMS messages, voice messages, and emails.

4.7.2.2 General Settings

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Enterprise Settings**.

Step 3 In the left-hand navigation pane, choose **General Settings**. On the displayed page, you will find options to configure the following items:

- Username Rule
When you or another administrator creates a user or imports identity source data, the username will be automatically populated with the corresponding letters in sequence. For example, if you input the username **Zhang San**, it will be displayed as **zhangsan** after the user is added. To enable this feature, you need to:
 - a. Select **Enable**.
 - b. Make the username field optional. Method: In the top navigation pane, choose **Users > User Attributes**. On the displayed page, click **Modify** in the **Operation** column of the **Username** field. In the displayed dialog box, deselect the **Required** checkbox in the **Field verification rules** setting.
 - c. Ensure that the username is empty when adding a user name by referring to [Creating a User](#).
- MFA Authentication
If you enable this option, you and other administrators need to enter a password and SMS verification code when logging in to the administrator portal.
- WeLink Authentication
If you enable this option and configure required parameters, you and other administrators can log in to the administrator portal through WeLink.

Table 4-29 Parameters

Parameter	Description
Client ID	Client ID of an application that you have created on the WeLink open platform.
Client Secret	Client secret of the application.
Callback URL	Callback address automatically generated by the platform, for example, https://xxx.huaweibccastle.com/api/ecb/welink/login . You can only view the callback address and cannot modify it.

 **NOTE**

Before you enable WeLink authentication in the administrator portal, ensure that you have created an application on the WeLink open platform.

- Identity Verification
 - **SMS:** Users will receive an SMS verification code during login, registration, and password resetting.
 - **DingTalk:** Users will receive a verification code sent by DingTalk during login, MFA, and password resetting. Ensure that you have configured the DingTalk gateway by referring to [DingTalk Gateway](#).

- Country Codes

After selecting **Country Codes**, you will then need to select a **Default Country Code**.

When a user enters a mobile number, they will see the available country codes to choose from. By default, the system automatically selects the default country code. If the default country code is not set, there is no need to select a country code when entering a mobile number. During the initial configuration of the default country code, the system will update any mobile numbers that do not include the default country code to include it.

Step 4 Click **Save**.

----End

4.7.2.3 User Agreement Configuration


You and other administrators can configure agreements and privacy statements on the OneAccess console. This ensures that users are fully aware of their rights and limitations when they first log in or register with the user portal.

Enabling and Configuring the User Agreement

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Enterprise Settings**.

Step 3 On the displayed page, choose **User Agreement Configuration**.

Step 4 (Optional) Click  to enable user agreement configuration.

 **NOTE**

By default, the user agreement configuration is disabled. Once this configuration is enabled, users will be required to check the service agreement and privacy terms during login or registration.

Step 5 Click **Modify** to set the agreement for different GUI languages.

1. Click the button to insert an agreement. In the displayed dialog box, enter the agreement name and text. Repeat this operation for different interface languages.
2. Click **OK**. The agreement name will be displayed in the text box, for example, **I have read and agree to the {Agreement name}**. You can click the agreement name in the text box to view its details.

 **NOTE**

You can insert up to 10 agreements at the same time.

Step 6 Click **Save** to finish the user agreement configuration.

----End

Modifying the User Agreement

 **NOTE**

Ensure that the user agreement configuration has been enabled.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Enterprise Settings**.

Step 3 On the displayed page, choose **User Agreement Configuration**.

Step 4 Click **Modify**.

Step 5 Click the agreement name in the text box. In the displayed dialog box, modify the agreement name and content.

Step 6 Click **OK**. The modified agreement name is displayed in the text box.

----End

Viewing Consented Users and Historical Agreement Versions

 **NOTE**

Ensure that you have configured user agreements.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Enterprise Settings**.

Step 3 On the displayed page, choose **User Agreement Configuration**.

Step 4 Click the agreement name to view the consented users and historical versions.

- The consented users tab allows you to see information about the users who have agreed to the terms, including the time of signing, username, name, version number, signing location, and signing result.
- The historical version tab allows you to see the agreement's version history, including the version numbers, number of consented users, effective date, and expiration date. You can click the view button in the **Operation** column to view historical agreements.

----End

Disabling the User Agreement Configuration


NOTE

Ensure that the user agreement configuration has been enabled.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Enterprise Settings**.

Step 3 On the displayed page, choose **User Agreement Configuration**.

Step 4 Click  to disable the user agreement configuration. Once this configuration is disabled, users will no longer need to check the service agreement and privacy terms during login or registration.

----End

4.7.2.4 SMS Gateway

The SMS gateway helps users receive SMS messages and verification codes, giving them the choice between a built-in gateway or a custom gateway.

When users purchase and create OneAccess instances, the SMS message limit is automatically set. By default, users can send up to 1,000 SMS messages per month for free cost. If more SMS messages are required, users can adjust the SMS gateway settings or contact technical support to increase the limit.

- Built-in gateway
 - The built-in gateway helps users obtain SMS messages and verification codes. On the **SMS Gateway** page, select **Built-in gateway**, and view the total and used SMS messages.
 - Check out the preset templates for different scenarios. In each situation, users will receive the preset SMS message or verification code.
 - To test the SMS message template for a specific scenario, click **Test** in the **Operation** column, specify a user, and click **Test**. Then check whether the user can receive the SMS message or verification code.
- Custom gateway

Register an account at the SMS service provider in advance and configure the gateway parameters in OneAccess. According to national message regulations, message template IDs and codes can be used only after the templates have been registered with and approved by the SMS service provider.

Supported SMS service providers include Huawei Cloud, Alibaba Cloud, and Horiz. Huawei Cloud is used for illustration.

- a. Log in to the administrator portal.
- b. On the top navigation bar, choose **Settings** > **Enterprise Settings**.
- c. On the **Enterprise Settings** page, choose **SMS Gateway** in the navigation pane. On the displayed page, select **Custom gateway** and set the basic parameters.

Table 4-30 Basic settings

Parameter	Mandatory	Description
SMS Service Provider	Yes	Select an SMS service provider, for example, Huawei Cloud .
Access Key ID	Yes	APP_Key of an SMS application created on the SMS service platform.
Access Key Secret	Yes	APP_Secret of the SMS application created on the SMS service platform.
Signature	Yes	Signature applied on the SMS service platform.
Verification Channel No.	Yes	Channel number generated when you apply for the verification signature on the SMS service platform.
Notification Channel No.	No	Channel number generated when you apply for the notification signature on the SMS service platform.
App Access Address	Yes	Access address of the SMS application created on the SMS service platform.

- d. In the **Scenarios** area, select a language, configure the template ID/code, and click **Save**.

 **NOTE**

The ID/code of each template must be the same as that of the template applied on the SMS service platform.

- e. (Optional) Click **Test** in the **Operation** column of the target scenario, specify a user, and click **Test** to check whether the SMS gateway configuration is successful.

4.7.2.5 Voice Gateway

The voice gateway helps users obtain voice verification codes. If a user cannot receive an SMS verification code, the user can choose to send a voice verification code instead. Either a built-in gateway or a custom gateway can be configured.

- Built-in gateway

- On the **Voice Gateway** page, select **Built-in gateway**, and view the total and used voice messages.
- Check out the preset voice message templates for different scenarios. In each situation, users will receive the preset voice message.
- To test the voice message template for a specific scenario, click **Test** in the **Operation** column, specify a user, and click **Test**. Then check whether the user can receive the voice message.
- Custom gateway
Register an account at the voice service provider and configure the gateway parameters in OneAccess. According to national message regulations, message template IDs and codes can be used only after the templates have been registered with and approved by the voice service provider. Supported voice service providers include Huawei Cloud and Alibaba Cloud.

This section uses Huawei Cloud to illustrate how to configure a voice gateway.

Prerequisites


The voice call service has been purchased.

Configuring Voice Gateway in OneAccess

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings** > **Enterprise Settings**.

Step 3 On the **Enterprise Settings** page, choose **Voice Gateway** in the left-hand

navigation pane. On the displayed page, click  to enable the voice gateway, select **Custom gateway**, and set the basic parameters.

Voice Gateway

Enable Voice Gateway Users can perform voice verification during login and registration

[Chinese Mainland](#)

Gateway Type Built-in gateway Custom gateway

Basic Settings

Voice Service Provider

* Access Key ID

* Access Key Secret

* App Access Address

* Display Number

Table 4-31 Basic settings

Parameter	Description
* Voice Service Provider	Select a voice service provider, for example, Huawei Cloud .
* Access Key ID	APP_Key of an application created on the voice service platform.
* Access Key Secret	APP_Secret of an application created on the voice service platform.
* App Access Address	Access address of the application created on the voice service platform.
* Display Number	Obtain it from the voice service platform.

Step 4 In the **Scenarios** area, select a language for messages, configure the template ID/code, and click **Save**.

Step 5 (Optional) Click **Test** in the **Operation** column of the target scenario, specify a user, and click **Test** to check whether the voice gateway configuration is successful.

----End

4.7.2.6 Email Gateway

The email gateway helps users obtain information through emails during password resetting. If you enable the email gateway, OneAccess will generate random passwords during password resetting and send them to users over email. The users can then use the received passwords to log in and set new passwords.

This section describes how to configure the email gateway in OneAccess.

Prerequisites

You have enabled the POP3/SMTP service. If not, go to the email account management page, enable POP3/SMTP service by following on-screen instructions, and save the authorization code.

NOTE

Keep your authorization code secure. If the authorization code is lost, generate a new one on the account setting page.

Configuring Email Gateway in OneAccess

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Enterprise Settings**.

Step 3 On the **Enterprise Settings** page, choose **Email Gateway** in the left-hand


navigation pane. On the displayed page, click  to enable the email gateway and set the basic parameters.

Table 4-32 Basic settings

Parameter	Mandatory	Description
SMTP HOST	Yes	Address of the host that provides SMTP services. You can find the value of this parameter in the documentation of the email gateway service platform.
SMTP Port	Yes	Port for providing SMTP services. The default port is 465.
Email Addresses	Yes	Enterprise email address, from which system emails will be sent.
Sender Name	Yes	Name of the email sender.
Authorization Code	Yes	Authorization code obtained in Prerequisites .
Security type	Yes	Email encryption mode, which must be the same as that specified on the email gateway service platform. You can find the value of this parameter in the documentation of the email gateway service platform. The default value is TLS. However, selecting SSL or not using any email encryption mode can potentially create security risks.

Step 4 (Optional) Click **Template Settings** and customize the email template.

----End

4.7.2.7 DingTalk Gateway

If SMS and voice verification codes fall short of your needs, you can configure the DingTalk gateway to send verification codes for various scenarios, such as user portal login, password recovery, two factor authentication, password resetting, and risk warning.

This section describes how to configure the DingTalk gateway in OneAccess.

Prerequisites

- You have administrator permissions for the DingTalk open platform. For details, see the documentation of the DingTalk open platform.
- You have permissions to access the administrator portal of OneAccess.

Configuring DingTalk Authentication in OneAccess

To ensure that a user can receive verification codes from DingTalk, configure a DingTalk authentication provider in OneAccess and bind the OneAccess user to DingTalk.

Creating a Mini App on the DingTalk Open Platform

You can create a mini app on the DingTalk open platform and grant API permissions to establish a connection between your app and the DingTalk authentication provider.

- Step 1** Log in to the DingTalk open platform.
 - Step 2** On the DingTalk open platform, choose **App Development > Organization Internal App > Mini App**, set app parameters, and click **Create**. The **AgentId**, **AppKey**, and **AppSecret** are automatically generated. For details, see the documentation of the DingTalk open platform.
 - Step 3** Go to the permission management area and add the API permission **Address book read-only**.
- End

Configuring DingTalk Gateway in OneAccess


- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Settings > Enterprise Settings**.
- Step 3** On the **Enterprise Settings** page, choose **DingTalk Gateway** in the left-hand navigation pane. On the displayed page, click  to enable the DingTalk gateway and set basic parameters.

Table 4-33 Basic settings

Parameter	Description
* Agent ID	AgentId of an app created on the DingTalk open platform.
* AppKey	AppKey of an app created on the DingTalk open platform.
* AppSecret	AppSecret of an app created on the DingTalk open platform.

- Step 4** (Optional) Click **Test** in the **Operation** column of the target scenario, specify a user, and click **Test** to check whether the DingTalk gateway configuration is successful.

 **NOTE**

If you see an error message stating that the verification code failed to be sent because the user is not bound to a DingTalk account, you will need to bind the DingTalk account by referring to [Configuring DingTalk Authentication in OneAccess](#).

Scenario	Template	Operation
Other	Verify Code \${param1}, it will expire in \${param2} minutes,please do not give to others.	Modify Test Copy
Reset Password	Username \${param1}, password \${param2}, please do not give to others.	Modify Test Copy
Risk Warning	Dear customer, we have detected your ccount "username \${param1}" is in risk,you can go to User Portal-Account Settings-Risk Event to che...	Modify Test Copy
Forgot Password	Verify Code \${param1}, it will expire in \${param2} minutes,please do not give to others.	Modify Test Copy
Login	Verify Code \${param1}, it will expire in \${param2} minutes,please do not give to others.	Modify Test Copy
MFA Authentication	Verify Code \${param1}, it will expire in \${param2} minutes,please do not give to others.	Modify Test Copy

----End

4.7.3 Dictionaries

Dictionaries enable you to efficiently manage business-related information, such as mobile numbers, state/province and city codes, and supplier regions. Dictionaries can be displayed in list and tree modes.

Adding a Dictionary


- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Settings > Dictionaries**.
- Step 3** On the **Dictionaries** page, click  at the bottom of the page.
- Step 4** In the **Add Dictionary** dialog box, enter dictionary information and click **Save**. The dictionary then appears in the list.

Table 4-34 Adding a dictionary

Parameter	Description
* Dictionary Code	The dictionary code must be unique. To facilitate dictionary management, set this parameter by following a unified rule.
* Dictionary Name	The dictionary name must be unique.
Tree Structure	Indicates whether to display the dictionary in list or tree mode. If you select this option, the dictionary is displayed in tree mode. Otherwise, the dictionary is displayed in list mode.
Description	Describes the usage and application scenarios of the dictionary.

- Step 5** Select a dictionary in the left pane.

 **NOTE**

- Dictionary items are subsets of a dictionary. Create a dictionary before adding dictionary items.
- Only dictionaries for which you have configured dictionary items can be used when you add custom user attributes.

- Step 6** On the right of the **Dictionaries** page, click **Add Dictionary Item**. In the displayed dialog box, enter the dictionary item information.

Table 4-35 Adding a dictionary item

Parameter	Description
* Dictionary Name	Parent node of the dictionary item. This parameter is not editable.
* Dictionary Item Code	Unique identifier of the dictionary item. To facilitate dictionary management, set this parameter by following a unified rule.
* Dictionary Item Name	Name of the dictionary item. Different dictionary items can have the same name.
Description	Describes the usage and application scenarios of the dictionary item.

Step 7 Click **Save**. The dictionary item then appears in the list.

----End


Modifying a Dictionary

If the user attribute associated with a dictionary changes, you can modify the dictionary to adapt for the change.

- Modifying a dictionary

 **NOTE**

The dictionary code and whether to display the dictionary in tree mode cannot be modified.

- Log in to the administrator portal.
- On the top navigation bar, choose **Settings > Dictionaries**.
- On the right side of the target dictionary, click  and select **Edit** from the drop-down list. The **Modify Dictionary** dialog box is displayed.
- Modify the dictionary name and description, and click **Save**.

 **NOTE**


The dictionary code and whether to display the dictionary in tree mode cannot be modified.

- Modifying a dictionary item
 - Log in to the administrator portal.
 - On the top navigation bar, choose **Settings > Dictionaries**.
 - Click the target dictionary. On the right side of the dictionary item list, click **Modify** in the **Operation** column of the dictionary item to be modified.
 - Modify the dictionary item name and description, and click **Save**.

Deleting a Dictionary

NOTE

Before you delete a dictionary, ensure that it is not associated with any user attributes.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Settings > Dictionaries**.
- Step 3** On the right side of the target dictionary, click  and select **Delete** from the drop-down list.
- Step 4** In the displayed dialog box, click **OK**.

----End

4.7.4 Data Import and Export

4.7.4.1 Importing Data

OneAccess allows you to effortlessly create users, organizations, and application accounts in batches by importing data.

NOTE

Ensure that the Excel file you upload is in the **.xlsx** format and has the same pattern as the template. The file must contain no more than 10,000 data items.

Users

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Settings > Import/Export**. By default, you are directed to the **Users** page.

NOTE

Before importing users, ensure that the organization for which you want to import users already exists. If the organization does not exist, add it by referring to [Adding an Organization](#). To add multiple organizations, see [Application Organizations](#).

- Step 3** Click **Download template**.
- Step 4** Open the downloaded Excel file, add user data to it, and save it.

NOTE

If the imported user belongs to multiple organizations, enter multiple organization codes and separate them with commas (.). By default, the first organization listed will be set as the primary organization.

- Step 5** On the **Users** page, click **Select File**, select the file saved in [Step 4](#), and click **Open**.
- Step 6** Click **Import** to import the user data.

----End

Organizations

1. Log in to the administrator portal.
2. On the top navigation bar, choose **Settings > Import/Export**. By default, you are directed to the **Users** page.
3. In the left-hand navigation pane, choose **Organizations**.
4. Click **Download template**.
5. Open the downloaded Excel file, add organization data to it, and save it.
6. On the **Organizations** page, click **Select File**, select the file saved in **5**, and click **Open**.
7. Click **Import** to import the organization data.

Application Accounts

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Settings > Import/Export**. By default, you are directed to the **Users** page.
- Step 3** In the left-hand navigation pane, choose **Application Accounts**.

 **NOTE**

Before importing application accounts, ensure that the application for which you want to import accounts already exists. For details about how to add an application, see [Adding an Application](#).

- Step 4** Click **Download template**.
- Step 5** Open the downloaded Excel file, add account data to it, and save it.
- Step 6** On the **Application Accounts** page, click **Select File**, select the file saved in **Step 5**, and click **Open**.
- Step 7** Click **Import** to import the application account data.

----End

Shared Accounts

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Settings > Import/Export**. By default, you are directed to the **Users** page.
- Step 3** In the left-hand navigation pane, choose **Shared Accounts**.

 **NOTE**

Before importing shared accounts, ensure that the application for which you want to import accounts already exists. For details about how to add an application, see [Adding an Application](#).

- Step 4** Click **Download template**.
- Step 5** Open the downloaded Excel file, add account data to it, and save it.

Step 6 On the **Shared Accounts** page, click **Select File**, select the file saved in **Step 5**, and click **Open**.

Step 7 Click **Import** to import the shared account data.

----End

Application Organizations

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Import/Export**. By default, you are directed to the **Users** page.

Step 3 In the left-hand navigation pane, choose **Application Organizations**.

NOTE

Before importing application organizations, ensure that the application to which the organizations to import will belong already exists. For details about how to add an application, see [Adding an Application](#).

Step 4 Click **Download template**.

Step 5 Open the downloaded Excel file, add application organization data to it, and save it.

Step 6 On the **Application Organizations** page, click **Select File**, select the file saved in **5**, and click **Open**.

Step 7 Click **Import** to import the application organization data.

----End

Application Resource Items

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Import/Export**. By default, you are directed to the **Users** page.

Step 3 In the left-hand navigation pane, choose **Application Resources Items**.

Step 4 Click **Download template**.

Step 5 Open the downloaded Excel file, add application resource items to it, and save it.

Step 6 On the **Application Resources Items** page, click **Select File**, select the file saved in **5**, and click **Open**.

Step 7 Click **Import** to import the application resource items.

----End

4.7.4.2 Exporting Data

Users

Step 1 Log in to the administrator portal.

- Step 2** On the top navigation bar, choose **Settings > Import/Export**. By default, you are directed to the **Users** page.
- Step 3** In the left-hand navigation pane, choose **Data Export > Users**.
- Step 4** Click **Export**. In the displayed dialog box, select **All** or **Specific** to specify the range of users you want to export.
- Step 5** Click **OK**. In the displayed **Security Authentications** dialog box, click **Get Code**, enter the verification code you received, and click **OK**.
- End

Organizations

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Settings > Import/Export**. By default, you are directed to the **Users** page.
- Step 3** In the left-hand navigation pane, choose **Data Export > Organizations**.
- Step 4** Click **Export**. In the displayed dialog box, select **All** or **Specific** to specify the range of organizations you want to export.
- Step 5** Click **OK**. In the displayed **Security Authentications** dialog box, click **Get Code**, enter the verification code you received, and click **OK**.
- End

4.7.5 UI Settings

You can customize the login, registration, and password recovery pages of the user portal for both PC and mobile devices. To customize the two pages, use the templates provided by OneAccess or add custom plans. In a custom template, you can modify the transparency, theme color, and content color of the top, form, and bottom areas. Moreover, you can customize the background image and the layout of the authentication window.

Global Settings

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Settings > UI Settings**.
- Step 3** Click **Global Settings** on the right. In the displayed dialog box, click **Modify** in the upper right corner to configure global parameters.

Table 4-36 Global settings

Global Parameter		Description
Basic Settings	Logo for Web	Enterprise logo displayed on the login page for PC. Upload a PNG, JPG, or GIF file whose size does not exceed 50 KB. The recommended image size is 42 × 180 pixels.

Global Parameter		Description
	Logo for Mobile	Enterprise logo displayed on the login page for mobile devices. Upload a PNG, JPG, or GIF file whose size does not exceed 50 KB. The recommended image size is 140 × 140 pixels.
	Favicon	Website icon. Upload an ICO file whose size does not exceed 5 KB. The recommended image size is 32 × 32 pixels.
User Portal Login Page	Man-Machine Verification	A two factor authentication method used on the login page. Currently, only slide puzzle verification is supported.
	Forgot Password	Configure whether to allow users to reset their passwords through the login page. By default, this option is enabled.
	Register	Configure whether to allow users to register accounts through the login page. By default, this option is disabled. NOTICE Once enabled, external users can register accounts. The new accounts will be associated with the root organization by default. Exercise caution when performing this operation.
	Text on the right side of the logo (Chinese)	The text is positioned to the right of the enterprise logo on the login/registration pages.
	Text on the right side of the logo (English)	The text is positioned to the right of the enterprise logo on the login/registration pages.
User Portal Homepage – Top Area	Background Color	Color in which the top area of the user portal homepage will be displayed.
	Font Color	Color of the text to be displayed at the top of the user portal homepage.
	Text on the right side of the logo (Chinese)	The text appears in the browser window and at the top of the user portal homepage.
	Text on the right side of the logo (English)	The text appears in the browser window and at the top of the user portal homepage.
Internationalization	Languages	Languages supported by the user portal.
	Default Language	Default language of the user portal.
Verification Code	Verification Code Length	Length of the verification code used for SMS verification in the user portal. Select either the 4-digit or 6-digit verification code.

Global Parameter		Description
	Validity Period	Validity period of the verification code used for SMS verification in the user portal. Set a validity period from 3 to 15 minutes.

Step 4 Click **Save**.

----End

User Portal for Web

Customize the login/registration web pages of the user portal for PC.



- User portal login page:
 - a. Log in to the administrator portal.
 - b. On the top navigation bar, choose **Settings > UI Settings**.
 - c. Choose **User Portal for Web > Customize User Portal Login Page**. On the displayed page, select a built-in template or configure a custom template.
 - In the **Built-in Templates** area, hover over a template, click , and select **Activate**. The template is set as the user portal login page.
 - In the **Custom Templates** area, click **Add Custom Plan** and set parameters by referring to [Table 4-37](#). To set the template as the login page for the user portal, click the button to save and activate it. To edit or delete a custom template, hover over it, click , and select **Modify** or **Delete**.

Table 4-37 Custom UI parameters

Area	Parameter	Description
UI layout	Layout template	Select a layout template.
	Background image	Background image of the user portal. The recommended image size is 1920 × 1080. Select a background image provided by the system or upload one.
	Background images	Background images provided by the system. Images you uploaded are also displayed in this area.
	Background color	Color of the background. NOTE The background image you select will cover the background color.

Area	Parameter	Description
Top Area	Display settings	Whether the top area of the user portal will be displayed. Select Display or Hide .
	Background Color	Background color of the top area in the user portal. Set this parameter only if you intend to display the top area.
	Content Color	Color of the text to be displayed in the top area of the user portal. Set this parameter only if you intend to display the top area.
Form Area	Form Position	Position of the login or registration form in the user portal. The options include Left , Center , and Right .
	Area color	You can configure the following options: <ul style="list-style-type: none"> • Background color: Color of the form area in the user portal. • Content color: Color of the text to be displayed in tab bars, form field labels, and other prompts. • Main color: Color of buttons in the form, tabs when they are selected or hovered over, and link text.
	Text field	Select a text box style. Then, specify the border and background color of the text boxes in the form area.
	Input	You can configure the following options: <ul style="list-style-type: none"> • Content color: Color of the text to be displayed in the form area. • Prompt color: Color of the prompt text to be displayed in the login form.
	Third-party login	You can configure the following options: Button border color, button background color, and content color.
Bottom Area	Display settings	Whether the bottom area of the user portal will be displayed. Select Display or Hide .

Area	Parameter	Description
	Background Color	Background color of the bottom area in the user portal. This parameter is available only for the login and registration page settings of the user portal for PC.
	Content Color	Color of the text to be displayed in the bottom area of the user portal.



- User portal registration page:
 - a. Log in to the administrator portal.
 - b. On the top navigation bar, choose **Settings > UI Settings**.
 - c. Choose **User Portal for Web > Customize User Portal Registration Page**. On the displayed page, select a built-in template or configure a custom template.
 - In the **Built-in Templates** area, hover over a template, click , and select **Activate**. The template is set as the registration page of the user portal.
 - In the **Custom Templates** area, click **Add Custom Plan** and set parameters by referring to [Table 4-38](#). To set the template as the registration page for the user portal, click the button to save and activate it. To edit or delete a custom template, hover over it, click , and select **Modify** or **Delete**.

Table 4-38 Custom UI parameters

Area	Parameter	Description
UI layout	Layout template	Select a layout template.
	Background image	Background image of the user portal. The recommended image size is 1920 × 1080. Select a background image provided by the system or upload one.
	Background images	Background images provided by the system. Images you uploaded are also displayed in this area.
	Background color	Color of the background. NOTE The background image you select will cover the background color.
Top Area	Display settings	Whether the top area of the user portal will be displayed. Select Display or Hide .

Area	Parameter	Description
	Background Color	Background color of the top area in the user portal. Set this parameter only if you intend to display the top area.
	Content Color	Color of the text to be displayed in the top area of the user portal. Set this parameter only if you intend to display the top area.
Form Area	Form Position	Position of the login or registration form in the user portal. The options include Left , Center , and Right . This parameter is available only for the login and registration page settings of the user portal for PC.
	Area color	You can configure the following options: <ul style="list-style-type: none"> • Background color: Color of the form area in the user portal. • Content color: Color of the text to be displayed in tab bars, form field labels, and other prompts. • Main color: Color of buttons in the form, tabs when they are selected or hovered over, and link text.
	Text field	Select a text box style. Then, specify the border and background color of the text boxes in the form area.
	Input	You can configure the following options: <ul style="list-style-type: none"> • Content color: Color of the text to be displayed in the form area. • Prompt color: Color of the prompt text to be displayed in the login form.
Bottom Area	Display settings	Whether the bottom area of the user portal will be displayed. Select Display or Hide .
	Background Color	Background color of the bottom area in the user portal.
	Content Color	Color of the text to be displayed in the bottom area of the user portal.

- User portal password recovery page:



- a. Log in to the administrator portal.
- b. On the top navigation bar, choose **Settings > UI Settings**.
- c. Choose **User Portal for Web** and go to the page for customizing the user portal password recovery page. Select a built-in template or configure a custom template.
 - In the **Built-in Templates** area, hover over a template, click , and select **Activate**. The template is set as the user portal password recovery page.
 - In the **Custom Templates** area, click **Add Custom Plan** and set parameters by referring to [Table 4-39](#). To set the template as the password recovery page for the user portal, click the button to save and activate it. To edit or delete a custom template, hover over it, click , and select **Modify** or **Delete**.


Table 4-39 Custom UI parameters

Area	Parameter	Description
UI layout	Layout template	Select a layout template.
	Background image	Background image of the user portal. The recommended image size is 1920 × 1080. Select a background image provided by the system or upload one.
	Background images	Background images provided by the system. Images you uploaded are also displayed in this area.
	Background color	Color of the background. NOTE The background image you select will cover the background color.
Top Area	Display settings	Whether the top area of the user portal will be displayed. Select Display or Hide .
	Background Color	Background color of the top area in the user portal. Set this parameter only if you intend to display the top area.
	Content Color	Color of the text to be displayed in the top area of the user portal. Set this parameter only if you intend to display the top area.
Form Area	Form Position	Position of the login or registration form in the user portal. The options include Left , Center , and Right .

Area	Parameter	Description
	Area color	You can configure the following options: <ul style="list-style-type: none"> • Background color: Color of the form area in the user portal. • Content color: Color of the text to be displayed in tab bars, form field labels, and other prompts. • Main color: Color of buttons in the form, tabs when they are selected or hovered over, and link text.
	Text field	Select a text box style. Then, specify the border and background color of the text boxes in the form area.
	Input	You can configure the following options: <ul style="list-style-type: none"> • Content color: Color of the text to be displayed in the form area. • Prompt color: Color of the prompt text to be displayed in the login form.
Bottom Area	Display settings	Whether the bottom area of the user portal will be displayed. Select Display or Hide .
	Background Color	Background color of the bottom area in the user portal.
	Content Color	Color of the text to be displayed in the bottom area of the user portal.

User Portal for Mobile

Customize the user portal login/registration pages for mobile devices such as mobile phones and tablets.

- User portal login page:
 - a. Log in to the administrator portal.
 - b. On the top navigation bar, choose **Settings > UI Settings**.
 - c. Choose **User Portal for Mobile > Customize User Portal Login Page**. On the displayed page, select a built-in template or configure a custom template.
 - In the **Built-in Templates** area, hover over a template, click , and select **Activate**. The template is set as the user portal login page.
 - In the **Custom Templates** area, click **Add Custom Plan** and set parameters by referring to [Table 4-40](#). To set the template as the


login page for the user portal, click the button to save and activate it. To edit or delete a custom template, hover over it, click , and select **Modify** or **Delete**.

Table 4-40 Custom UI parameters

Area	Parameter	Description
UI layout	Layout template	-
	Background image	Background image of the user portal. The recommended image size is 1920 × 1080. Select a background image provided by the system or upload one.
	Background images	Background images provided by the system. Images you uploaded are also displayed in this area.
	Background color	Color of the background. NOTE The background image you select will cover the background color.
Top Area	Display settings	Whether the top area of the user portal will be displayed. Select Display or Hide .
	Background Color	Background color of the top area in the user portal. Set this parameter only if you intend to display the top area.
	Content Color	Color of the text to be displayed in the top area of the user portal. Set this parameter only if you intend to display the top area.
	logo setting	Whether the enterprise logo will be displayed in top area of the user portal. Select Display or Hide .
Form Area	Area color	You can configure the following options: <ul style="list-style-type: none"> • Background color: Color of the form area in the user portal. • Content color: Color of the text to be displayed in tab bars, form field labels, and other prompts. • Main color: Color of buttons in the form, tabs when they are selected or hovered over, and link text.

Area	Parameter	Description
	Text field	Specify the border color of the text boxes in the form area.
	Input	You can configure the following options: <ul style="list-style-type: none"> Content color: Color of the text to be displayed in the form area. Prompt color: Color of the prompt text to be displayed in the login form.
Bottom Area	Display settings	Color of the text to be displayed in the bottom area of the user portal.
	Bottom Font	Text to be displayed in the bottom area of the user portal.



- User portal registration page:
 - a. Log in to the administrator portal.
 - b. On the top navigation bar, choose **Settings > UI Settings**.
 - c. Choose **User Portal for Mobile > Customize User Portal Registration Page**. On the displayed page, select a built-in template or configure a custom template.
 - In the **Built-in Templates** area, hover over a template, click , and select **Activate**. The template is set as the registration page of the user portal.
 - In the **Custom Templates** area, click **Add Custom Plan** and set parameters by referring to [Table 4-41](#). To set the template as the registration page for the user portal, click the button to save and activate it. To edit or delete a custom template, hover over it, click , and select **Modify** or **Delete**.

Table 4-41 Custom UI parameters

Area	Parameter	Description
UI layout	Layout template	Select a layout template.
	Background image	Background image of the user portal. The recommended image size is 1920 × 1080. Select a background image provided by the system or upload one.
	Background images	Background images provided by the system. Images you uploaded are also displayed in this area.

Area	Parameter	Description
	Background color	Color of the background. NOTE The background image you select will cover the background color.
Top Area	Background Color	Background color of the top area in the user portal. Set this parameter only if you intend to display the top banner.
	Content Color	Color of the text to be displayed in the top area of the user portal. Set this parameter only if you intend to display the top banner.
Form Area	Area color	Main color: Color of buttons in the form, tabs when they are selected or hovered over, and link text.
	Text field	Specify the border color of the text boxes in the form area.
	Input	You can configure the following options: <ul style="list-style-type: none"> Content color: Color of the text to be displayed in the form area. Prompt color: Color of the prompt text to be displayed in the login form.

4.7.6 Service Settings

OneAccess can interconnect with applications through OAuth2, SAML, OIDC, and CAS. It also provides OTP services. View the parameters of these services when you interconnect OneAccess with different applications.

Configuring OTP

An OTP is generated by a virtual MFA device in compliance with the Time-based One-time Password Algorithm (TOTP) standard. MFA devices can be hardware- or software-based. Currently, OneAccess only supports software-based virtual MFA devices, which are application programs running on mobile devices such as smart phones.

OneAccess supports OTP configuration. You can also configure the OTP parameters to your virtual MFA device. For details, see the documentation of the virtual MFA device.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Service Settings**.

- Step 3** On the **Service Configuration** page, click **OTP**. In the displayed dialog box, set the following parameters.

Table 4-42 Parameter configuration

Parameter	Description
Encryption Algorithm	Default algorithm: HMACSHA1. This parameter can be modified.
Code Digits	Default value: 6. This parameter cannot be modified.
Generation Period (s)	Default value: 30. This parameter cannot be modified.
Time Offset	Default value: 0. This parameter can be modified.
Base Time	Default value: GMT. This parameter cannot be modified.
MFA Authentication with Password	If you enable this option, users need to enter an OTP code in addition to their usernames and passwords during OTP login. By default, this option is disabled.

- Step 4** Click **Save** to complete the OTP configuration.

----End

 **NOTE**

To use OTP login for an application, ensure that you have enabled OTP authentication for PC or mobile devices on the login configuration page of the application.

Configuring IDP

To establish a SAML-based trust relationship with an application, upload the metadata of the IDP to the SP server. For details about how to upload the metadata, see the documentation provided by the SP.

- Step 1** Log in to the administrator portal.
- Step 2** On the top navigation bar, choose **Settings > Service Settings**.
- Step 3** On the **Service Configuration** page, click **IdP**. In the displayed dialog box, set the following parameters.

Table 4-43 IdP service parameters

Parameter	Description
IdP EntityId	Unique identifier of the IDP.
SSO URL	URL for SSO.
IdP Logout URL	URL for SLO.

Parameter	Description
IdP Certificate	A public key certificate used for signature verification. The signing certificate in the metadata file is used by applications during user access to ensure that assertions are credible and complete.
Assertion Request Time Window	Default value: 2 minutes. You can select a different value from the drop-down list. The value ranges from 1 to 5 minutes.
Session Validity Period	Default value: 30 minutes. The value ranges from 1 to 480.
Request Signature	By default, this option is enabled.
Assertion Signature	By default, this option is enabled.
Assertion Encryption	By default, this option is enabled.

Step 4 Click **Download IdP Metadata** in the upper right corner to save and upload the data to the SP server.

Step 5 Click **Save**.

----End

Configuring OIDC

To establish an OIDC- or OAuth2-based trust relationship with an application, obtain the required port information.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Service Settings**.

Step 3 On the **Service Configuration** page, click **OIDC**. In the displayed dialog box, view the following parameters.

Parameter	Description
Authentication URL	Interface for authenticating users during application access. The default value is used.
Token URL	Interface for obtaining user tokens. The default value is used.
User Information	Only the default value can be used.
Refresh Token URL	Interface for refreshing user tokens. The default value is used.

Step 4 Click **OIDC Settings** in the upper right corner to download OIDC data.

----End

Configuring CAS

To establish a CAS-based trust relationship with an application, view and configure CAS information.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Service Settings**.

Step 3 On the **Service Configuration** page, click **CAS**. In the displayed dialog box, view and modify the following parameters.

Table 4-44 Parameter description

Parameter	Description
Server Prefix	Prefix of the CAS server URL. The value is automatically generated by the system and cannot be modified.
Login URL	URL for CAS request authorization. The URL is automatically generated by the system and cannot be modified.
Validate URL V3	URL for ticket verification. V3 URL is recommended. The URL is automatically generated by the system and cannot be modified.
Logout URL	URL for logging out of CAS. The URL is automatically generated by the system and cannot be modified.
ST Validity Period	Validity period of a returned ST. Set a validity period from 3 to 15 minutes.

Step 4 Click **Save**.

----End

Configuring API Authentication

To register open APIs with OneAccess, view the API authentication settings and configure them for interaction with your applications.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Settings > Service Settings**.

Step 3 On the **Service Configuration** page, click **API Authentication**. In the displayed dialog box, view the following parameters.

Parameter	Description
Signature Algorithm	Only the default value can be used.

Parameter	Description
Public Key	Public key for signature verification. Only the default value can be used.
Encryption Algorithm	Only the default value can be used.
Algorithm Key	Key used by the encryption algorithm. Click Reset to set a key.
Validity Period	Validity period of access_token and id_token . The default value is 30 minutes. You can adjust this period up to a maximum of 43200 minutes (30 days).

----End

4.7.7 CloudBridge Agent Configuration

CloudBridge agents establish a network security tunnel between the internal services of your enterprise and OneAccess. This prevents your internal services from being exposed to the public network and protects network entities from interception and repeated attacks.

Currently, CloudBridge Agents support the AD identity source as well as the AD and LDAP authentication providers. This section describes how to connect AD and LDAP to OneAccess through CloudBridge Agents.

Prerequisites

Ensure that you have the capabilities required to deploy CloudBridge agents.

Obtaining the CloudBridge Software Packages

Table 4-45 CloudBridge software packages

Software Package Name	How to Obtain
cloudAgent-*.zip	<ul style="list-style-type: none"> CloudBridge identity source package: https://oneaccess-cn-east-3-obs.obs.cn-east-3.myhuaweicloud.com/cloudbridge/cloudAgent-identitySource-24.5.1.1.zip Verification file of the CloudBridge identity source package: https://oneaccess-cn-east-3-obs.obs.cn-east-3.myhuaweicloud.com/cloudbridge/cloudAgent-identitySource-24.5.1.1.zip.sha256 CloudBridge authentication provider package: https://oneaccess-cn-east-3-obs.obs.cn-east-3.myhuaweicloud.com/cloudbridge/cloudAgent-authSource-24.5.1.1.zip Verification file of the CloudBridge authentication provider package: https://oneaccess-cn-east-3-obs.obs.cn-east-3.myhuaweicloud.com/cloudbridge/cloudAgent-authSource-24.5.1.1.zip.sha256

 **NOTE**

The download links of CloudBridge packages do not contain **sha256**. Links that end with **sha256** are used to download software package verification files.

Checking the Update Logs of the CloudBridge Deployment Package

The following table lists the update logs of the CloudBridge deployment package.

Version	What's New
V24.5.1.1	Upgraded the JDK version to 17.
V23.12.1.1	Resolved some known issues.
V23.6.1.0	Added support for random numbers, which are more secure.
V23.2.1.0	Added support for the LDAP authentication provider and optimized startup logs.
V22.11.1.0	Added signature verification and optimized log printing.
V22.6.1.0	Added the function for administrators to view CloudBridge client run logs in the administrator portal.
V22.3.1.0	Optimized the AD identity source agent.

Version	What's New
V21.9.2.0	Added the watchdog mechanism.
V21.9.1.0	1. Optimized the CloudBridge reconnection mechanism. 2. Resolved some known issues.

Verifying the Integrity of the CloudBridge Agent Software Package

NOTE

The software package version number mentioned in this document is just an example.

- Step 1** Use PuTTY or FTP to connect to the server to be deployed. Then, log in to the server as the **root** user, and use SFTP to upload the CloudBridge Agent software package and the corresponding SHA-256 file to the server. Next, run **ll** to view the uploaded software package and verification file.

```
[root@cluster-test-eq9ku xxx]# ll
total 75724
-rw-r--r-- 1 root root 32696037 Dec 1 16:12 cloudAgent-authSource-24.5.1.1.zip
-rw-r--r-- 1 root root 101 Dec 1 16:11 cloudAgent-authSource-24.5.1.1.zip.sha256
-rw-r--r-- 1 root root 44832098 Dec 1 16:12 cloudAgent-identitySource-24.5.1.1.zip
-rw-r--r-- 1 root root 105 Dec 1 16:11 cloudAgent-identitySource-24.5.1.1.zip.sha256
```

- Step 2** Run the following commands to check the integrity of the gateway software package. If **OK** is displayed, the package is complete.

sha256sum -c cloudAgent-identitySource-24.5.1.1.zip.sha256

```
[root@cluster-test-eq9ku xxx]# sha256sum -c cloudAgent-identitySource-24.5.1.1.zip.sha256
cloudAgent-identitySource-24.5.1.1.zip: OK
```

sha256sum -c cloudAgent-authSource-24.5.1.1.zip.sha256

```
[root@cluster-test-eq9ku xxx]# sha256sum -c cloudAgent-authSource-24.5.1.1.zip.sha256
cloudAgent-authSource-24.5.1.1.zip: OK
```

NOTE

If the integrity check fails, the software package might have been damaged during the download process. Download the software package again or contact technical support.

----End

Procedure

- Step 1** Deploy the AD service, and create a domain account to establish an enterprise management system. For details, see [Setting Up an AD Server](#) and [Creating a Domain Account](#).
- Step 2** Add a CloudBridge agent.
1. Log in to the administrator portal.
 2. On the top navigation bar, choose **Settings > CloudBridge Agents**.
 3. On the **CloudBridge Agents** page, click **Add CloudBridge Agent**. Then, enter an agent name, select either **Authentication Provider** or **Identity Source** for the CloudBridge agent type, and click **OK**.



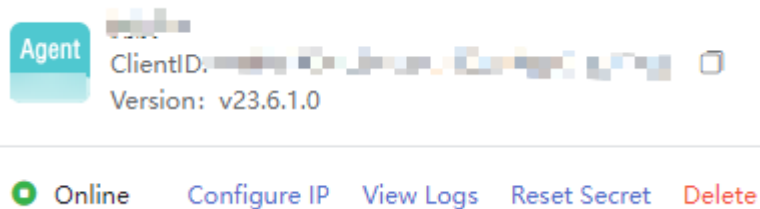
Offline [Configure IP](#) [View Logs](#) [Reset Secret](#) [Delete](#)

NOTE

- The system automatically generates a client ID and secret for the CloudBridge agent you created. Keep the client ID and secret properly.
- If you have forgotten the client secret, click **Reset Secret** to generate a new one for the target agent. The original secret will become invalid after the resetting. Exercise caution when performing this operation.
- Click **Configure IP** to configure the IP address of the server where the CloudBridge Agent is located. If this parameter is left unconfigured, IP address access control will be disabled. Only one IP address can be configured, and IP addresses using an asterisk (*) as a wildcard (for example, **10.10.10.***) are not supported. Only the CloudBridge Agent set up on the specified IP address will be accessible.
- To view the connection logs, click **View Logs**.
- To delete the CloudBridge agent, click **Delete**.

Step 3 Deploy the CloudBridge agent. If the deployment is successful, the agent status is displayed as **Online** on the **CloudBridge Agents** page.

Figure 4-7 Viewing CloudBridge agent status



The following instructions explain how to deploy the CloudBridge Agents of the identity source and the authentication provider type.

 NOTE

- The server must have JDK 17 installed. (For versions earlier than CloudBridge 24.5.1.1, JRE 1.8 is required.)

1. Download the JDK source code package from the official website.
2. Run the following commands to extract the JRE to the specified directory and configure the JRE environment variables:

```
tar -zxvf jdk-17_linux-x64_bin.tar.gz -C /usr/local/
chmod 755 /usr/local/jdk-17.0.12
echo "export PATH" >> /etc/profile
echo "export PATH=$PATH:/usr/local/jdk-17.0.12/bin" >> /etc/profile
source /etc/profile
java -version
```

- The server must have curl and netstat installed to use the watchdog function.
- You are advised to run the CloudBridge client as a non-root user.

If a non-root user already exists, you do not need to create one. If you prefer to use a new non-root user, run the following commands as the **root** user:

```
groupadd {User group}
useradd -d /home/Username -s /bin/bash -g User group -m Username
unzip -od {Directory where the decompressed files are stored} cloudAgent.zip
chown -R {Username}:{User group} {Directory where the decompressed files are stored}
chmod 700 -R {Directory where the decompressed files are stored}
su - {Username}
```

- The following procedure uses CentOS Linux release 8.2.2004 as an example to describe how to deploy the CloudBridge identity source agent.
 - a. Download the deployment package of the identity source agent according to the region where the instance is located.
 - b. Upload the deployment package to the target server.
 - c. Run **unzip -od {Directory where the decompressed files are stored} cloudAgent.zip** to decompress the deployment package. Specify a unique directory to ensure successful deployment. For details about the deployment package, see [Table 4-46](#).

Table 4-46 Directory structure

Name	Description
agent.sh	Automatically runs the agent upon startup.
cloudAgent-identitySource.jar	Serves as the agent deployment package.
cloudBridge.sh	Used to manually run the agent.
config	Serves as the directory for storing the agent configuration file (application.yml).
connector	Serves as the deployment package of the LDAP connector.

Name	Description
encrypt.sh	Used to encrypt the passwords of principal accounts in AD.
log	Serves as the directory for storing the agent log file (agent.log).

- d. Go to the directory where the decompressed files are stored, and configure the **application.yml** file in the **config** directory. Add a space in front of each attribute value. For details about the parameters involved, see [Adding an AD Identity Source in OneAccess](#).

To encrypt **agentSecret** and **credentials**, follow these steps:

- i. Generate the root key and working key. Run the **./encrypt.sh setKey** command in the directory where the CloudBridge installation package is decompressed. When prompted with the message "please enter the encryption key:", enter your custom key and press **Enter**. If you see the message "the encryption key setting succeeds", the key has been set successfully.
- ii. Run the **./encrypt.sh encrypt** command. When prompted with the message "please enter what you want to encrypt content:", enter the value of **agentSecret** and press **Enter** to obtain the encrypted **agentSecret**, for example, **{AES_GCM}0000xxxxxx111111**.
- iii. Run the **./encrypt.sh encrypt** command. When prompted with the message "please enter what you want to encrypt content:", enter the value of **credentials** and press **Enter** to obtain the encrypted **credentials**, for example, **{AES_GCM}0000xxxxxx222222**.
- iv. Copy the encrypted value into the appropriate position in the **application.yml** file. Enclose the value in double quotation marks ("").

```

server:
  address: 127.0.0.1
  port: 2341

agent:
  # This is the connection address of the agent
  # env:
  # http://domaincontroller.com/api/v1/wg
  serverAddress: http://192.168.1.100.com/api/v1/wg
  # This is the client id of the agent
  clientId: 98765432109876543210987654321098
  # This is the client secret of the agent
  agentSecret: " {AES_GCM}0000xxxxxx111111 "
  # This is the identity source reclaim attribute
  idsource:

replay:
  # This is the AD identity source reclaim attribute
  ad:
    # Host name or IP address of the AD server
    host: 192.168.1.100
    # IP or port used to communicate with the AD server
    port: 389
    # Select this check box to connect to the AD server using SSL.
    ssl: false
    # Whether to enable startTLS for encryption. StartTLS and SSL can't be set true at same time.
    startTLS: false
    # TLSv1.2 is used by default, and TLSv1.3 and TLSv1.2 are recommended. SSL and TLSv1.0 can be used for compatibility.
    protocolVersion: TLSv1.2
    # Determine whether to verify certificate when ssl is true or startTLS is true.
    verifyingCertificate: true
  # Identity source authentication
  principal:
    # Password for the principal
    password: " {AES_GCM}0000xxxxxx222222 "
    # One or more starting points in the LDAP tree that will be used when searching the LDAP tree.
    # A search is performed when a user is found from the LDAP server or when the group to which a user belongs.
    baseContexts:

```

Table 4-47 Parameter description

Parameter	Description
* address	Listening address for CloudBridge startup. The default value is 127.0.0.1 .

Parameter	Description
* port	The listening port for CloudBridge startup can be modified. Assign different port numbers when starting multiple CloudBridge agents. The default value is 9081 .
* serverAddress	wss://{Domain name of the tenant who needs to use the CloudBridge agent}/api/v1/ws
* agentId	Automatically generated by the system after the agent is added. For details, see Step 2 .
* agentSecret	Automatically generated by the system after the agent is added. For details, see Step 2 .
* host	IP address of the AD server.
* port	TCP/IP port of the AD server.
* ssl	The default value is true , indicating that SSL is used for connecting to the AD server. If you do not want to use SSL, set the value to false .
* principal	Identifier used for AD server authentication.
* credentials	Password of principal .
* baseContexts	The root node (for example, OU=huaweitest,DC=test,DC=com) in the AD tree where the accounts to be synchronized are located.

 NOTE

If you do not receive any responses after running the `./encrypt.sh setKey` command and entering a key, install the `rng-tools` to enhance the rate at which the system entropy pool is replenished.

1. Run the following commands to install `rng-tools`:

```
yum install rng-tools
```

```
cat /etc/sysconfig/rngd
```

If the file does not exist, run the following command to add it:

```
echo "OPTIONS=\"-r /dev/urandom\"" > /etc/sysconfig/rngd
```

2. Run the following commands to start the `rng` service and query its status:

```
service rngd start: starts the rng service.
```

```
service rngd status: checks the rng service status.
```

If the status is **enabled**, the service is actively running.

```
root@oneaccess ~]# service rngd status
Redirecting to /bin/systemctl status rngd.service
● rngd.service - Hardware RNG Entropy Gatherer Daemon
   Loaded: loaded (/usr/lib/systemd/system/rngd.service; enabled; vendor preset: enabled)
   Active: active (running) since 2024-12-26 10:10:10 CST; 1min 45s ago
     Main PID: 29323 (rngd)
    CGroup: /system.slice/system-hostos.slice/rngd.service
            └─29323 /sbin/rngd -f
```

- e. Once you finish the configuration, run the **./cloudBridge.sh start** command to start the agent. If you see the message "Starting Agent Success.", the agent startup is successful.

 **NOTE**

- Ensure that you have permissions for the deployment package.
 - The message "Starting Agent Fail." indicates that the startup fails. Check the configuration file.
 - To enable automatic startup, run the **./agent.sh install** command as the **root** user. This installation process also verifies the basic system environment to ensure that all service installation requirements are met. You will be prompted to enter the startup user during the installation. If no startup user is specified, the script will be run with the current user. If you see the message "The Agent service installed successfully, need to reboot will take effect.", the installation is successful.
 - To uninstall the agent, run **./agent.sh uninstall**. The message "uninstall Agent Success." shows up, indicating that the agent is uninstalled successfully.
 - If you do not receive any response after running the command **./cloudBridge.sh start**, you can install rng-tools by following the instructions in the previous section where a similar problem occurs after running **./encrypt.sh setKey**.
- f. Obtain logs from the **log/agent.log** file.
- The following procedure uses CentOS Linux release 8.0.1905 as an example to describe how to deploy the CloudBridge authentication provider agent.
 - a. Download the deployment package of the authentication provider agent according to the region where the instance is located.
 - b. Upload the deployment package to the target server.
 - c. Run **unzip -od {Directory where the decompressed files are stored} cloudAgent.zip** to decompress the deployment package. Specify a unique directory to ensure successful deployment. For details about the deployment package, see [Table 4](#).

Table 4-48 Directory structure

Name	Description
agent.sh	Automatically runs the CloudBridge agent upon startup.
cloudAgent-authSource.jar	Serves as the agent deployment package.
cloudBridge.sh	Used to manually run the agent.
config	Serves as the directory for storing the agent configuration file (application.yml).
log	Serves as the directory for storing the agent log file (agent.log).

- d. Go to the directory where the decompressed files are stored, and configure the **application.yml** file in the **config** directory. Add a space in front of each attribute value.

Table 4-49 Parameter description

Parameter	Description
* address	Listening address for CloudBridge startup. The default value is 127.0.0.1 .
* port	The listening port for CloudBridge startup can be modified. Assign different port numbers when starting multiple CloudBridge agents. The default value is 9082 .
* serverAddress	wss://{Domain name of the tenant who needs to use the CloudBridge agent}/api/v1/ws
* agentId	Automatically generated by the system after the CloudBridge agent is added. For details, see Step 2 .
* agentSecret	Automatically generated by the system after the CloudBridge agent is added. For details, see Step 2 .
* urls	Address of the AD server. To obtain this parameter, see Adding an AD Authentication Provider .
* rootDn	AD node used to authenticate users. To obtain this parameter, see Adding an AD Authentication Provider .
* domain	If the tenant domain name contains the AD domain name, set this parameter to the AD domain name. Otherwise, do not set this parameter.
* searchFilter	Query condition. To obtain this parameter, see Adding an AD Authentication Provider .
* urls	LDAP address. To obtain this parameter, see Adding an LDAP Authentication Provider .
sslCheck	Whether to perform LDAPS SSL check: If this parameter is not configured or set to true , the SSL certificate will be verified. If the SSL certificate does not need to be checked, set this parameter to false .
* baseDn	Base DN of a user. To obtain this parameter, see "Adding an LDAP Authentication Provider in OneAccess".
managerDn	Identifier of the administrator. The default value is cn=Directory Manager .
managerPassword	ID of the LDAP administrator account.

Parameter	Description
userSearchBase	Search path for LDAP users. To obtain this parameter, see Adding an LDAP Authentication Provider .
userSearchFilter	Filter conditions for matching system users in LDAP. The default value is (&(objectClass=user)(uid={0})) . For details, see LDAP Filters . DN-based query takes priority over condition-based query.
dnPatterns	Search path for LDAP users. The default value is uid={0},ou=people . DN authentication takes priority over other authentication modes.

 NOTE

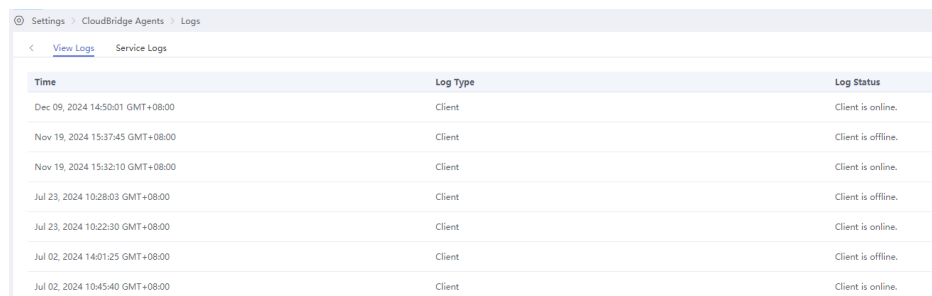
You can encrypt **agentSecret** by referring to [Step 3.d](#).

- e. Once you finish the configuration, run the **./cloudBridge.sh start** command to start the agent. If you see the message "Starting Agent Success.", the agent startup is successful.

 NOTE

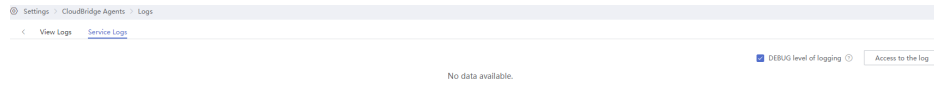
- Ensure that you have permissions for the deployment package.
 - The message "Starting Agent Fail." indicates that the startup fails. Check the configuration file.
 - To enable automatic startup, run the **./agent.sh install** command as the **root** user. This installation process also verifies the basic system environment to ensure that all service installation requirements are met. You will be prompted to enter the startup user during the installation. If no startup user is specified, the script will be run with the current user. If you see the message "The Agent service installed successfully, need to reboot will take effect.", the installation is successful.
 - To uninstall the agent, run **./agent.sh uninstall**. The message "uninstall Agent Success." shows up, indicating that the agent is uninstalled successfully.
- f. Obtain logs from the **log/agent.log** file.

Step 4 Click **View Logs**. By default, the connection logs tab is displayed. You can view the time when CloudBridge goes online or offline.



Time	Log Type	Log Status
Dec 09, 2024 14:50:01 GMT+08:00	Client	Client is online.
Nov 19, 2024 15:37:45 GMT+08:00	Client	Client is offline.
Nov 19, 2024 15:32:10 GMT+08:00	Client	Client is online.
Jul 23, 2024 10:28:03 GMT+08:00	Client	Client is offline.
Jul 23, 2024 10:22:30 GMT+08:00	Client	Client is online.
Jul 02, 2024 14:01:25 GMT+08:00	Client	Client is offline.
Jul 02, 2024 10:45:40 GMT+08:00	Client	Client is online.

Step 5 Click **Service Logs**. On the displayed page, you can view CloudBridge startup logs in real time.



Step 6 Add an AD identity source, an AD authentication provider, and an LDAP authentication provider.

1. Add an AD identity source.

- a. Log in to the administrator portal.
- b. On the top navigation bar, choose **Users > Identity Sources**.
- c. On the **Identity Sources** page, click **Add Identity Source** in the **Operation** column of the row that contains **AD**, enter an identity source name, and click **OK**.

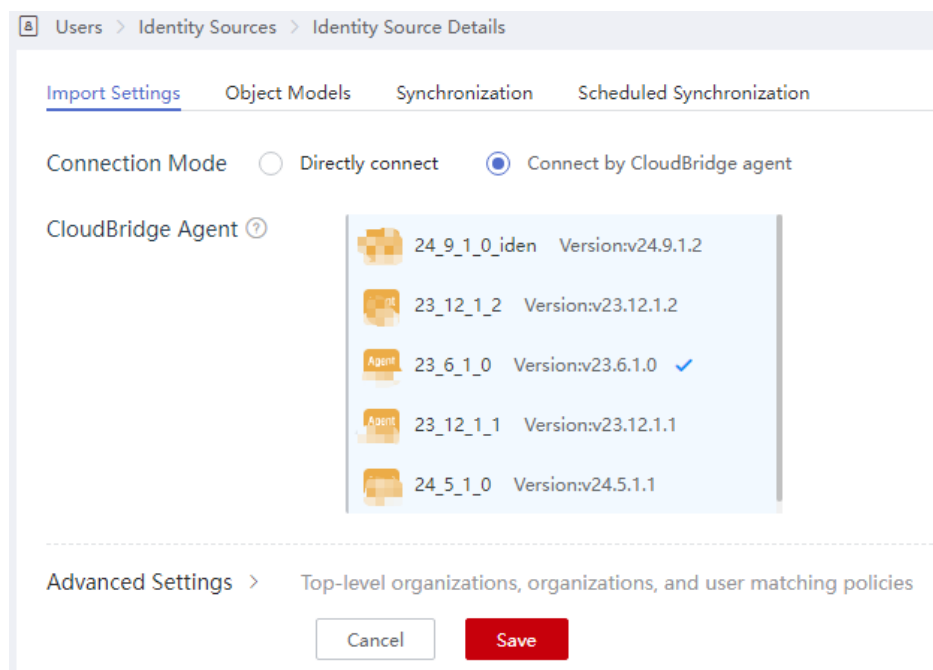
The screenshot shows the 'Identity Sources' page. It includes a breadcrumb 'Users > Identity Sources' and a title 'Identity Sources'. Below the title is an information box stating: 'Various identity sources are supported for importing users and organizations. You can flexibly configure the import data processing logic to aggregate the identity data from multiple identity sources into a user directory. Some identity sources support real-time synchronization with a callback URL.' Below this is a table with the following data:

Identity Source Type	Supported Objects	Description	Operation
DingTalk	Users & organizations	Synchronize data from DingTalk.	Add Identity Source
WeCom	Users & organizations	Synchronize data from WeCom.	Add Identity Source
Feishu	Users & organizations	Synchronize data from Feishu.	Add Identity Source
AD	Users & organizations	Synchronize data from AD.	Add Identity Source
LDAP	Users & organizations	Synchronize data from LDAP.	Add Identity Source

- d. In the AD identity source list, click **View Details** in the row that contains the target identity source. On the displayed **Import Settings** page, set **Connection Mode** to **Connect by CloudBridge agent** and select the added CloudBridge agent. Up to five CloudBridge agents can be selected. For details about advanced settings and object models, see [Adding an AD Identity Source](#).

The screenshot shows the 'Identity Sources' page with the same table as above. The 'AD' row has a red box around the 'View Details' link. Below the table is a detailed view for the 'AD' identity source:

Identity Source Name	Status	Operation
AD	Pending	View Details Delete

Figure 4-8 Configuring import/export

- e. Synchronize data. For details, see [Verifying Synchronization of AD Data](#).
2. Add an AD authentication provider.
 - a. Log in to the administrator portal.
 - b. On the top navigation bar, choose **Authentication > Authentication Providers**. Then click **AD**.
 - c. On the **AD Authentication Providers** page, click **Add Authentication Provider** in the upper right and set the required parameters.

Figure 4-9 Adding an AD authentication provider

Add Authentication Provider ✕

* Display Name

Connection Mode Directly connect Connect by CloudBridge agent

CloudBridge Agent ?

Agent	24_5_1_1	Version:v24.5.1.1	✓
Agent	24_9_1_0	Version:v24.9.1.2	
Agent	██████	Version:v23.6.1.0	
Agent	██████	Version:v23.6.1.0	
Agent	██████	Version:v23.6.1.0	

* Source Attribute ?

* Related User Attribute ?

No User Associated ?

AD Configuration Test

Account	<input type="text" value="Account Name"/>	Password	<input style="border: none; padding: 2px 5px;" type="text" value="Account Password"/>
---------	---	----------	---

Please enter your test account

🕒 Connection test has not started yet.

Table 4-50 Parameter description

Parameter	Description
* Display Name	Display name of the authentication provider, for example, AD .
* Connection Mode	Select Connect by CloudBridge agent .
* CloudBridge Agent	Select the CloudBridge agent added in Step 2 . You can select a maximum of five CloudBridge agents.
* Source Attribute	AD user attribute, for example, sAMAccountName .

Parameter	Description
* Related User Attribute	The only text type attribute, such as userName , to map the AD user attribute.
* No User Associated	Operation that will be performed if a user logs in successfully but fails to be associated with a system user.
* Update Existing Attribute	Determine whether to update the existing user attribute value when a user logs in successfully through AD and is associated with a system user.

To map other attributes, such as **name**, set **No User Associated** to **Automatically create users**, and click **Add Mapping** to add the desired mappings. For details, see [Table 4-51](#).

Table 4-51 Mapping parameters

Parameter	Description
User Attribute	Attribute in OneAccess to which AD will map. For example, email .
Mapping Type	How user attributes are mapped between OneAccess and AD. For example, Authentication Provider Attribute .
Authentication Provider Attribute Name	Name of an AD user attribute.

- d. Enter a test account and password and click **Test** to check the connectivity.

If you have selected multiple (up to 5) CloudBridge agents when adding an AD authentication provider, the system checks the connectivity of each agent after you click **Test**. If the check fails, view the cause.
 - e. Enable AD authentication for an application. For details, see [Enabling AD Authentication in OneAccess](#).
 - f. Verify login using an AD account. For details, see [Logging In to the User Portal Through AD Authentication](#).
3. Add an LDAP authentication provider.
 - a. Log in to the administrator portal.
 - b. On the top navigation bar, choose **Authentication > Authentication Providers**. Then click **LDAP**.
 - c. On the **LDAP Authentication Providers** page, click **Add Authentication Provider** in the upper right corner and set the parameters required.

Table 4-52 Parameter description

Parameter	Description
* Display Name	Display name of the authentication provider, for example, LDAP .
* Connection Mode	Select Connect by CloudBridge agent .
* CloudBridge Agent	Select the CloudBridge agent added in Step 2 . You can select a maximum of five CloudBridge agents.
* Source Attribute	LDAP user attribute, for example, sAMAccountName .
* Related User Attribute	The only text attribute, such as userName , to map the LDAP user attribute.
* No User Associated	Operation that will be performed if a user logs in successfully but fails to be associated with a system user.
* Update Existing Attribute	Determine whether to update the existing user attribute value when a user logs in successfully through LDAP and is associated with a system user.

To map other attributes, such as name, set **No User Associated** to **Automatically create users**, and click **Add Mapping** to add the desired mappings. For details, see [Table 4-53](#).

Table 4-53 Mapping parameters

Parameter	Description
User Attribute	Attribute in OneAccess to which LDAP will map. For example, email .
Mapping Type	How user attributes are mapped between OneAccess and LDAP. For example, Authentication Provider Attribute .
Authentication Provider Attribute Name	Name of an LDAP user attribute.

- d. Enter a test account and password and click **Test** to check the connectivity.

If you have selected multiple (up to 5) CloudBridge agents when adding an LDAP authentication provider, the system checks the connectivity of each agent after you click **Test**. If the check fails, view the cause.

- e. Enable LDAP authentication. For details, see [Enabling LDAP Authentication](#).
- f. Verify login through LDAP authentication. For details, see [Logging In to the User Portal Through LDAP Authentication](#).

----End

5 Common User Guide

5.1 Registering an Account

You can log in to the user portal **as a user** that has been created by the administrator. If you do not have an account, follow the instructions in this section to register one.

Prerequisites

The administrator has enabled user account registration. For details, see [Global Settings](#).

Procedure

Step 1 Go to the user portal login page.

 **NOTE**

Obtain the user portal URL from the enterprise administrator. For example, **https://example.huaweioneaccess.com**.

Step 2 Click **Register now** on the login page.

User Login

[SMS](#) [OTP](#) [Password](#)

+86 Input mobile

Input verification code [Send Code](#)

Remember me

[Login](#)

[Register now](#) [Forgot password](#)

Login With



We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.[Learn More](#)

Step 3 Enter a mobile number on the registration page.

The screenshot shows a 'Sign up' page with a header 'Have an account? Login now'. Below the header is a form with a dropdown menu for the country code (set to '+86') and a text input field for the mobile number. Below the mobile number field is a text input field for the verification code and a 'Send Code' button. At the bottom of the form is a large blue 'Next' button.

Step 4 Click **Send Code** and enter the verification code you received into the designated text box.

Step 5 Click **Next**, enter a username, and set and confirm the password.

NOTE

The administrator determines the user information that needs to be entered by [setting the user attributes](#) used for registration information collection.

Step 6 (Optional) Select the [user agreement enabled and configured](#) by the administrator.

NOTE

When registering an account, you are required to select the user agreement that has been configured and enabled. For details, see [Enabling and Configuring the User Agreement](#).

Step 7 Click **Save**. Once registered, you can access the user portal using the account.

NOTE

By default, the new account is assigned to the root organization. If you want to select your desired organization during account registration, contact the administrator to enable organization configuration. For details, see [Modifying User Attributes](#).

----End

5.2 Resetting a Password

If you forget your password, you can reset it on the user portal login page.

Prerequisites

The administrator has enabled user password resetting. For details, see [Global Settings](#).

Procedure

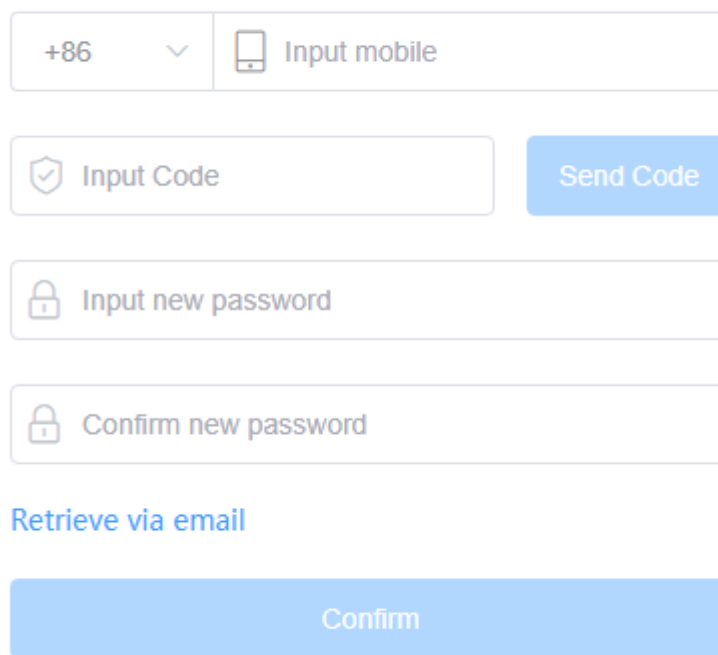
Step 1 Go to the user portal login page.

 **NOTE**

Obtain the user portal URL from the enterprise administrator. For example, **https://example.huaweioneaccess.com**.

Step 2 On the login page, click **Forgot password**. The **Find Password** page is displayed. By default, mobile number verification is used for password resetting.

Find Password



The screenshot shows the 'Find Password' interface. It features a mobile number input field with a dropdown menu set to '+86' and a placeholder 'Input mobile'. Below this is a verification code input field with a shield icon and a 'Send Code' button. Further down are two password input fields, both with lock icons and placeholders 'Input new password' and 'Confirm new password'. At the bottom, there is a blue 'Confirm' button and a 'Retrieve via email' link.

[Back](#)

Step 3 You have two verification options to reset your password:

- Mobile number verification
 - a. Enter your mobile number and click **Send Code**.
 - b. Enter the received verification code.
 - c. Enter a new password and confirm it.
 - d. Click **Confirm**. You can now log in to the user portal using your new password.
- Email verification
 - a. Enter your email address and click **Send Code**.
 - b. Enter the received verification code.
 - c. Enter a new password and confirm it.

- d. Click **Confirm**. You can now log in to the user portal using your new password.

----End

5.3 Logging In to the User Portal and Accessing Applications

5.3.1 SMS

Prerequisites

- You have a user portal account. If not, contact your enterprise administrator to create one for you. Alternatively, you can register an account on the user portal by referring to [Registering an Account](#).
- The administrator has enabled SMS authentication for application login on the user portal. For details, see [Login Configuration](#).
- The administrator has configured the SMS gateway. For details, see [SMS Gateway](#).

Procedure

Step 1 Go to the user portal login page.

 **NOTE**

Obtain the user portal URL from the enterprise administrator. For example, <https://example.huaweioneaccess.com>.

Step 2 On the login page, click the **SMS** tab and enter a mobile number.

User Login

SMS

OTP

Password

Remember me

[Register now](#)

[Forgot password](#)

Login With



We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.[Learn More](#)

Step 3 Click **Send Code** and enter the received verification code in the text box. If you select **Remember me**, you do not need to enter the mobile number the next time you log in.

NOTE

If you do not receive the SMS message, try the voice verification code. This option is only available if the administrator has configured the voice gateway. For details, see [Voice Gateway](#).

Step 4 Click **Login**.

Step 5 (Optional) Select the [user agreement enabled and configured](#) by the administrator and log in.

 **NOTE**

- When logging in to the user portal for the first time, you are required to select the user agreement that has been configured and enabled. For details, see [Enabling and Configuring the User Agreement](#).
- If the administrator has modified the user agreement, you must select the updated agreement the next time you log in. For details, see [Modifying the User Agreement](#).

Step 6 On the user portal homepage, click the logo of the application you want to access.

----End

5.3.2 OTP

Prerequisites

- You have a user portal account. If not, contact your enterprise administrator to create one for you. Alternatively, you can register an account on the user portal by referring to [Registering an Account](#).
- The administrator has enabled OTP-based authentication for application login on the user portal. For details, see [Login Configuration](#).
- The administrator has configured the OTP. For details, see [Configuring OTP](#).
- You have enabled OTP-based authentication on the user portal. For details, see [Account Security](#).

Procedure

Step 1 Go to the user portal login page.

 **NOTE**

Obtain the user portal URL from the enterprise administrator. For example, <https://example.huaweioneaccess.com>.

Step 2 Select **OTP** on the login page.

User Login

SMS

OTP

Password



Input username, or email address



OTP after user account activated.

Use Mobile Number

 Remember me

Login

[Register now](#)[Forgot password](#)

Login With



We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.[Learn More](#)

- By default, you need to provide your username/email address, and enter the OTP you receive.
- Alternatively, select **Use Mobile Number** to receive the OTP through your mobile.

Step 3 Select **Remember me** as needed. Click **Login**.

Step 4 (Optional) Select the **user agreement enabled and configured** by the administrator and log in.

NOTE

- When logging in to the user portal for the first time, you are required to select the user agreement that has been configured and enabled. For details, see [Enabling and Configuring the User Agreement](#).
- If the administrator has modified the user agreement, you must select the updated agreement the next time you log in. For details, see [Modifying the User Agreement](#).

Step 5 On the user portal homepage, click the logo of the application you want to access.

----End

5.3.3 Password

Prerequisites

- You have a user portal account. If not, contact your enterprise administrator to create one for you. Alternatively, you can register an account on the user portal by referring to [Registering an Account](#).
- The administrator has enabled password-based authentication for application login on the user portal. For details, see [Login Configuration](#).

Procedure

Step 1 Go to the user portal login page.

 **NOTE**

Obtain the user portal URL from the enterprise administrator. For example, <https://example.huaweioneaccess.com>.

Step 2 Select **Password** on the login page.

User Login

SMS

OTP

Password



Input username, or email address



Input password

Use Mobile Number

Remember me

Login

[Register now](#)

[Forgot password](#)

Login With



We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.[Learn More](#)

- By default, you need to provide your username/email address and password.
- Alternatively, select **Use Mobile Number**. Then, provide your mobile number and password.

Step 3 Select **Remember me** as needed. Click **Login**.

Step 4 (Optional) Select the **user agreement enabled and configured** by the administrator and log in.

NOTE

- When logging in to the user portal for the first time, you are required to select the user agreement that has been configured and enabled. For details, see [Enabling and Configuring the User Agreement](#).
- If the administrator has modified the user agreement, you must select the updated agreement the next time you log in. For details, see [Modifying the User Agreement](#).

Step 5 On the user portal homepage, click the logo of the application you want to access.

----End

5.3.4 Authentication Provider


You can log in to the user portal using an authentication provider. For details, see [Authentication Provider](#).

 NOTE

- When using the authentication provider to log in to the user portal for the first time, you are required to select the user agreement that has been configured and enabled. For details, see [Enabling and Configuring the User Agreement](#).
- If the administrator has modified the user agreement, you must select the updated agreement the next time you log in with the authentication provider. For details, see [Modifying the User Agreement](#).

User Login

SMS OTP Password

 Input username, or email address

 Input password

Use Mobile Number

Remember me

Login

[Register now](#)

[Forgot password](#)

Login With



We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.[Learn More](#)

5.4 Account Delegation

Overview

With account delegation, you can temporarily authorize an account to redirect to an application associated with your own account. This grants the delegated account access to the application on your behalf. Once the delegation period ends, the delegated account will no longer have access to the application. This feature enhances both account security and convenience.

Prerequisites

- Delegating account: has an application that can be redirected to, and can log in to the OneAccess user portal.
- Delegated account: can log in to the OneAccess user portal.

Delegating Application Access on the User Portal

Step 1 Log in to the OneAccess user portal.

Step 2 Click **Account Entrusted**.

Step 3 In the displayed dialog box, select the application you want to authorize access for, specify the delegated user, enter a description, and set the desired delegation period.

Step 4 Click **OK**.

----End

Accessing Applications with a Delegated Account

Step 1 Log in to the OneAccess user portal using a delegated account.

Step 2 On the user portal homepage, click the icon of the application that you have been granted access to.

 **NOTE**

If your delegated account has had the permission to access the application, you can choose to access this application using the original permission or the delegated permission.

----End

5.5 Account Settings

In the user portal, view and modify your personal information and manage your account security settings.

Viewing and Modifying Personal Information

In the upper right corner of the user portal, click the user profile and select **Account Settings**. On the displayed **Personal Information** page, you can view and modify basic information.

NOTE

The enterprise administrator configures whether to allow specific users to view and modify their personal information. To change your permissions on the personal information, contact the enterprise administrator.

Risky Events

In the upper right corner of the user portal, click the user profile and select **Account Settings**. On the displayed **Personal Information** page, choose **Risk Events** in the left-hand navigation pane. On the displayed page, specify a period and select a risk type to view risk event details.

Account Security

In the upper right corner of the user portal, click the user profile and select **Account Settings**. On the displayed **Personal Information** page, choose **Account Security** in the left-hand navigation pane. On the displayed page, you can change the login password, bind a mobile number to your account, and enable OTP-based authentication.

- **Password:** Change the login password of your account.
- **Mobile Number:** Change the mobile number associated with your account.
- **OTP Authentication:** An OTP is in compliance with the TOTP standard.

a. Bind your account.

Open your WeChat and search for **OTP** in mini programs. For example, open the mini program of Bamboocloud and click the button to scan the QR code.

b. Enter the OTP generated by the mini program.

c. Confirm your operation to enable OTP-based authentication.

NOTE

If the QR code cannot be scanned, open the OTP mini program and enter the account name and key.

Shared Accounts

If you have been specified as the controller of an application account, manage users of the account on the **Shared Account** page.

For details about how to add a shared account, see [Authorization Management](#).

Statistics

In the upper right corner of the user portal, click the user profile and select **Account Settings**. On the displayed **Personal Information** page, choose **Statistics**

in the left-hand navigation pane. On the displayed page, you can view your frequently accessed applications, frequent locations, authentication statistics, frequently used authentication types, authentication failure causes, and frequently used devices.

Operation Logs

In the upper right corner of the user portal, click the user profile and select **Account Settings**. On the displayed **Personal Information** page, choose **Operation** in the left-hand navigation pane. On the displayed page, you can view your operation logs. Query operation logs by time, operation type, resource type, or operation result.

6 Key Operations Recorded by CTS

6.1 OneAccess Operations Recorded by CTS

Cloud Trace Service (CTS) is a log audit service provided by Huawei Cloud and intended for cloud security. It collects and stores cloud resource operation records, and allows you to query them for security analysis, auditing, resource change tracking, and fault locating.

To view key OneAccess operations, such as certificate updates, [enable CTS](#).

CTS will then record your operations on the OneAccess console. [Table 1](#) shows the OneAccess operations that can be recorded by CTS.

Table 6-1 OneAccess operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Buying an instance	instance	orderInstance
Updating a certificate	certificate	updateCertificate
Creating a custom domain name	domainName	createDomainName
Deleting a custom domain name	domainName	deleteDomainName
Deleting an instance	instance	deleteInstance

6.2 Viewing CTS Traces in the Trace List

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in Object Storage Service (OBS) buckets. Cloud Trace Service (CTS) stores operation records (traces) generated in the last seven days.

NOTE

These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.


This section describes how to query or export operation records of the last seven days on the CTS console.




- [Viewing Real-Time Traces in the Trace List of the New Edition](#)
- [Viewing Real-Time Traces in the Trace List of the Old Edition](#)

Constraints


- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, you must configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console one minute later and query data traces five minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.



Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
 - **Trace Name:** Enter a trace name.
 - **Trace ID:** Enter a trace ID.
 - **Resource Name:** Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.

- **Resource ID:** Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
 - **Trace Source:** Select a cloud service name from the drop-down list.
 - **Resource Type:** Select a resource type from the drop-down list.
 - **Operator:** Select one or more operators from the drop-down list.
 - **Trace Status:** Select **normal**, **warning**, or **incident**.
 - **normal:** The operation succeeded.
 - **warning:** The operation failed.
 - **incident:** The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
 - **Enterprise Project ID:** Enter an enterprise project ID.
 - **Access Key:** Enter a temporary or permanent access key ID.
 - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
- Enter any keyword in the search box and press **Enter** to filter desired traces.
 - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
 - Click  to view the latest information about traces.
 - Click  to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled () , excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see [Trace Structure](#) and [Example Traces](#).
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available.
 - **Trace Type, Trace Source, Resource Type, and Search By:** Select a filter from the drop-down list.

- If you select **Resource ID** for **Search By**, specify a resource ID.
 - If you select **Trace name** for **Search By**, specify a trace name.
 - If you select **Resource name** for **Search By**, specify a resource name.
 - **Operator**: Select a user.
 - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
 - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
6. Click **Query**.
 7. On the **Trace List** page, you can also export and refresh the trace list.
 - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
 - Click  to view the latest information about traces.
 8. Click  on the left of a trace to expand its details.

Trace Name	Resource Type	Trace Source	Resource ID	Resource Name	Trace Status	Operator	Operation Time	Operation
createDockerConfig	dockerlogincmd	SWR	-	dockerlogincmd	normal		Nov 16, 2023 10:54:04 GMT+08:00	View Trace

request

trace_id: [redacted]

code: 200

trace_name: createDockerConfig

resource_type: dockerlogincmd

trace_rating: normal

api_version: [redacted]

message: createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason: [redacted]

source_ip: [redacted]

domain_id: [redacted]

trace_id: [redacted]

trace_type: ApiCall

9. Click **View Trace** in the **Operation** column. The trace details are displayed.

View Trace ×

```

{
  "request": "",
  "trace_id": "[redacted]",
  "code": "200",
  "trace_name": "createDockerConfig",
  "resource_type": "dockerlogincmd",
  "trace_rating": "normal",
  "api_version": "",
  "message": "createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:",
  "source_ip": "[redacted]",
  "domain_id": "[redacted]",
  "trace_type": "ApiCall",
  "service_type": "SWR",
  "event_type": "system",
  "project_id": "[redacted]",
  "response": "",
  "resource_id": "",
  "tracker_name": "system",
  "time": "Nov 16, 2023 10:54:04 GMT+08:00",
  "resource_name": "dockerlogincmd",
  "user": {
    "domain": {
      "name": "[redacted]",
      "id": "[redacted]"
    }
  }
}

```

10. For details about key fields in the trace structure, see [Trace Structure](#) and [Example Traces](#) in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.