OneAccess

User Guide

Issue 04

Date 2021-08-17



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. 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 Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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 Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Before You Start..... 1

2 Enterprise Administrator Guide..... 2

2.1 Logging In to Administrator Portal..... 2
2.2 User Management..... 3
2.2.1 Users..... 3
2.2.2 Organizations..... 10
2.2.3 User Groups..... 14
2.2.4 Identity Sources..... 16
2.2.5 User Attributes..... 21
2.3 Resources..... 24
2.3.1 Overview..... 24
2.3.2 Adding an Application..... 25
2.3.3 Configuring an Application..... 30
2.3.4 Enabling or Disabling an Application..... 44
2.3.5 Deleting an Application..... 45
2.3.6 Authorizing Access to Built-in APIs..... 46
2.3.7 Calling Built-in APIs..... 50
2.3.8 Modifying Built-in APIs..... 51
2.3.9 Adding a Custom API..... 52
2.3.10 Configuring a Custom API..... 52
2.3.11 Deleting a Custom API..... 53
2.3.12 Adding an Enterprise Device..... 53
2.3.13 Modifying Device Information..... 56
2.3.14 Deleting an Enterprise Device..... 58
2.4 Authentication..... 58
2.4.1 Authentication Providers..... 58
2.4.2 Regions..... 60
2.5 Security..... 62
2.5.1 Administrator Permissions..... 62
2.5.2 Password Policy..... 68
2.6 Auditing..... 69
2.6.1 OneAccess Auditing..... 69
2.6.2 HUAWEI CLOUD Auditing..... 70

 Copyright © Huawei Technologies Co., Ltd.

2.7 Settings 72
2.7.1 Enterprise Information 72
2.7.2 Enterprise Settings 73
2.7.3 Dictionaries 78
2.7.4 Data Import 81
2.7.5 UI Configuration 84
2.7.6 Service Configuration 88
2.7.7 CloudBridge Agent Configuration 91
3 Common User Guide 99
3.1 Logging In to OneAccess and Accessing Applications 99
3.2 Account Settings 100
4 Change History 103

 Copyright © Huawei Technologies Co., Ltd.

1 Before You Start

Intended Audience

- 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**.

 Copyright © Huawei Technologies Co., Ltd.

2 Enterprise Administrator Guide

Logging In to Administrator Portal

User Management

Resources

Authentication

Security

Auditing

Settings

2.1 Logging In to Administrator Portal

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

Prerequisites

- You have registered a HUAWEI CLOUD account and completed real-name authentication.
- You have purchased an instance.

If the preceding operations are not completed, **purchase an instance** now.

Procedure

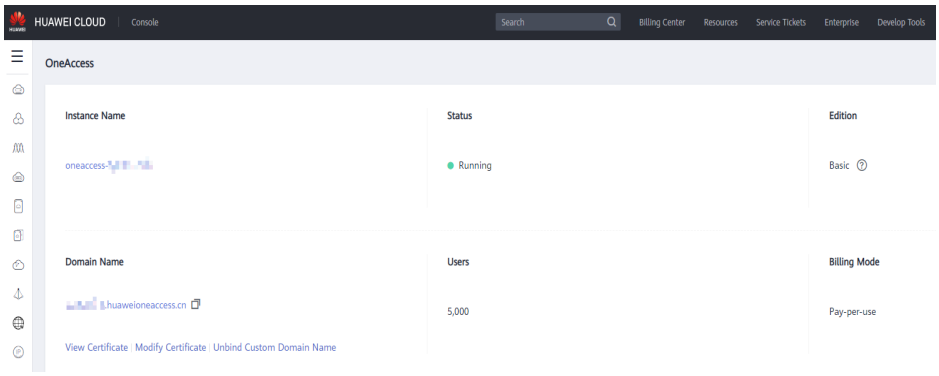
Step 1 Log in to the HUAWEI CLOUD management console.

Step 2 Choose **Service List** > **Management & Governance** > **OneAccess** to go to the OneAccess console.

Step 3 Click the instance name to go to the administrator portal.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-1 Clicking the instance name



----End

2.2 User Management

2.2.1 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.

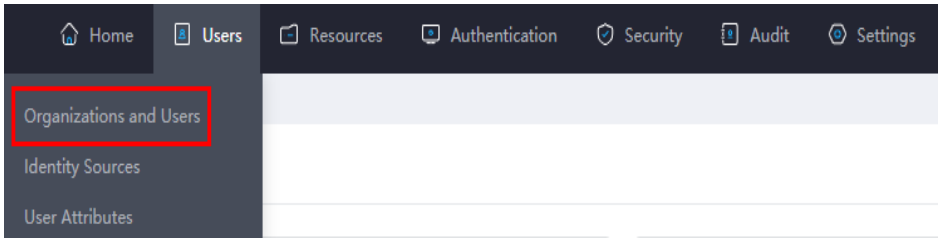
- Import from identity sources: Configure data import logic to synchronize identity data from upstream identity sources to OneAccess. For details, see **Identity Sources**.
- Import with a template: Add user data to the template and then import the user data to OneAccess. For details, see **Importing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

Creating a User

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Users** > **Organizations and Users**.

Figure 2-2 Organizations and Users

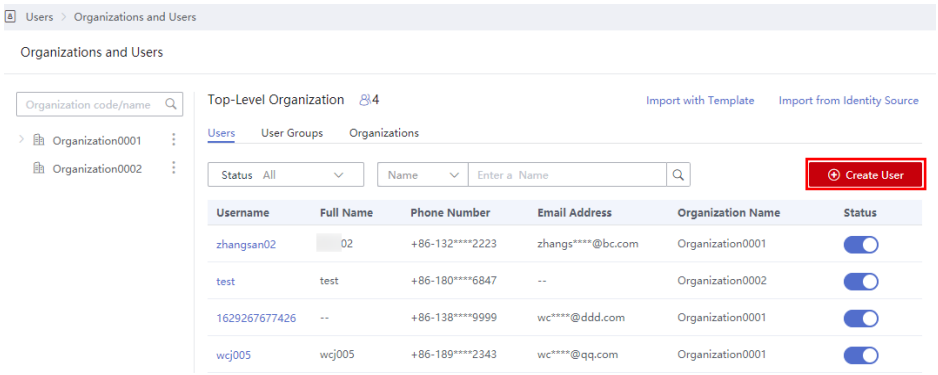


Step 3 On the **Organizations and Users** page, click the **Users** tab.

Step 4 In the left organization tree, select an organization to which you want to create a user, and click **Create User**. For details about how to create an organization, see **Adding an Organization**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-3 Creating a user



NOTE

- If no username is specified, the system automatically generates a username.
- The username, mobile number, and email address of the user cannot be the same as those of other users.
- The user can log in to the user portal using their username, mobile number, or email address.
- If you reset the user's password, a password reset 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 login authentication mode is enabled.
- User information includes basic and extended attributes. Set attributes on the **User Attributes** page. For details, see **User Attributes**.

Step 5 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**.

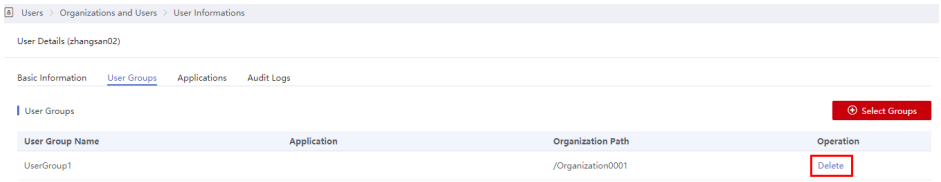
Figure 2-4 Select Groups



 Copyright © Huawei Technologies Co., Ltd.

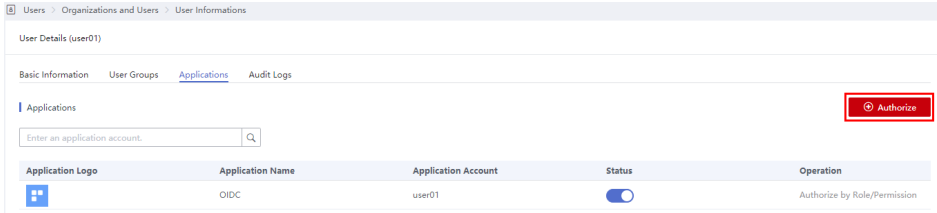
  - To remove the user from a user group, click **Delete** in the **Operation** column of the row that contains the group.

    Figure 2-5 Removing a user from a user group

- 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**.

    Figure 2-6 Authorize

  - 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

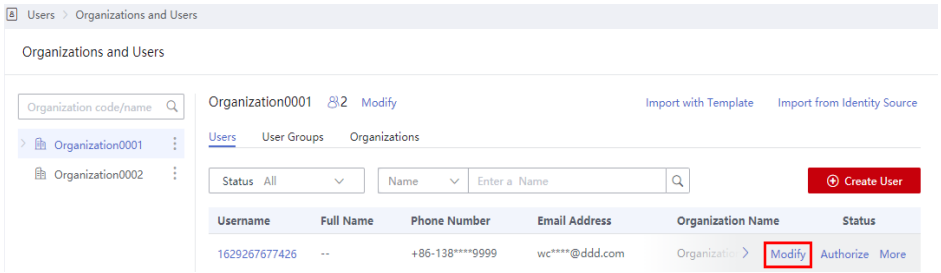
    Administrators' operations on the user, such as changing the password and authorizing application access. Set filter conditions to view desired logs.
  - User logs

    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

In the user list, click **Modify** in the row that contains the target user, and modify the basic and extended attributes.

Figure 2-7 Modifying user information

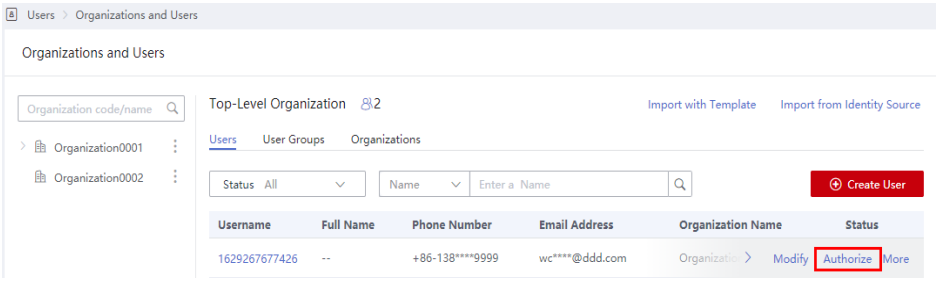


 Copyright © Huawei Technologies Co., Ltd.

Granting Application Access to a User

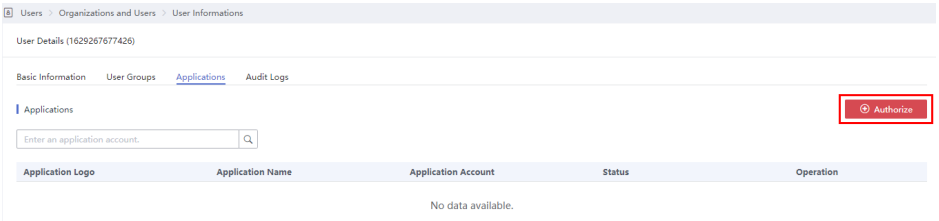
Step 1 In the user list, click **Authorize** in the row that contains the target user. To add an application, see **Application Integration**.

Figure 2-8 Clicking Authorize



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

Figure 2-9 Authorizing application access



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.

Figure 2-10 Setting account names



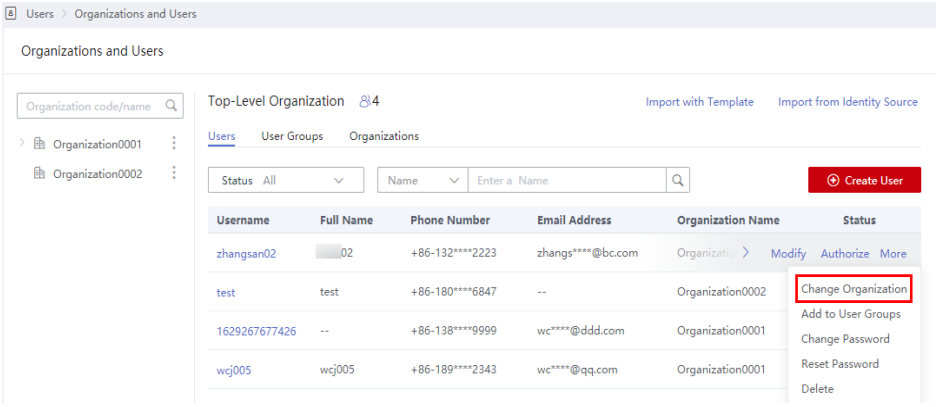
----End

Changing the Organization of a User

Step 1 In the user list, choose **More** > **Change Organization** in the row that contains the target user.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-11 Changing the organization



Step 2 Select the target organization to which the user will belong.

Step 3 Click **OK**.

NOTE

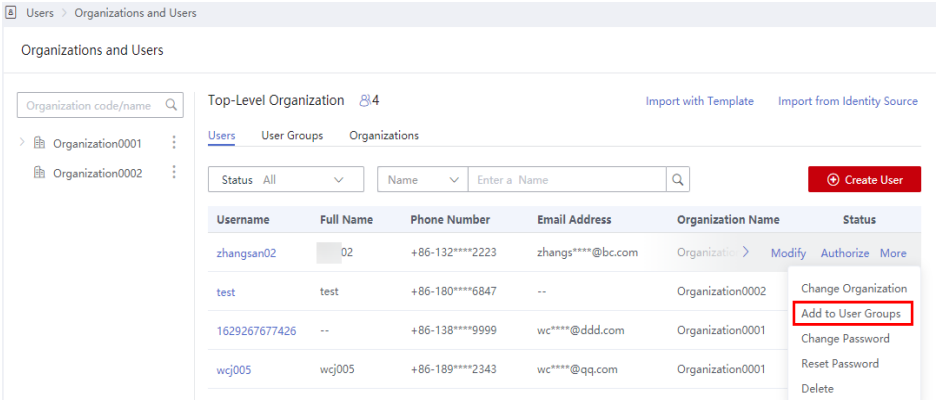
If you have enabled **automatic user authorization** for an application, changing the organization of a user will change the user's access to the application.

----End

Adding a User to One or More User Groups

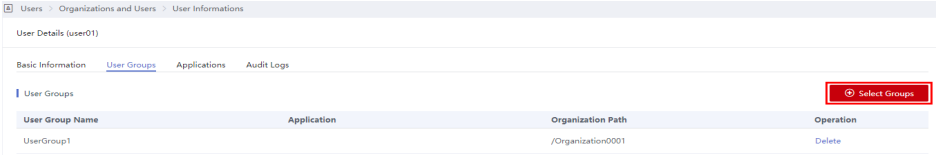
Step 1 In the user list, choose **More** > **Add to User Groups** in the row that contains the target user.

Figure 2-12 Add to User Groups



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

Figure 2-13 Select Groups



 Copyright © Huawei Technologies Co., Ltd.

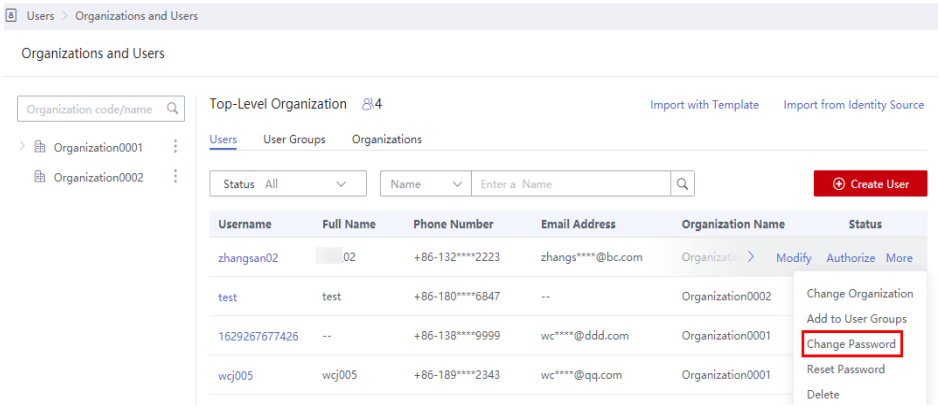
Step 3 Select user groups to which the user will belong, and click **Save**. To remove the user from a user group, click **Delete** in the **Operation** column of the row that contains the group.

----End

Changing the Password of a User

Step 1 In the user list, choose **More** > **Change Password** in the row that contains the target user.

Figure 2-14 Changing the password



Step 2 Enter a new password and enter it again. To require the user to change the password at first login to the user portal, select **Require password reset**.

Step 3 Click **OK**.

----End

Resetting the Password of a User

After you reset the password of a user, the user will be notified by email, SMS, or DingTalk based on the notification method you select. The user can then use the new password to log in to the user portal. The following procedure uses SMS as an example.

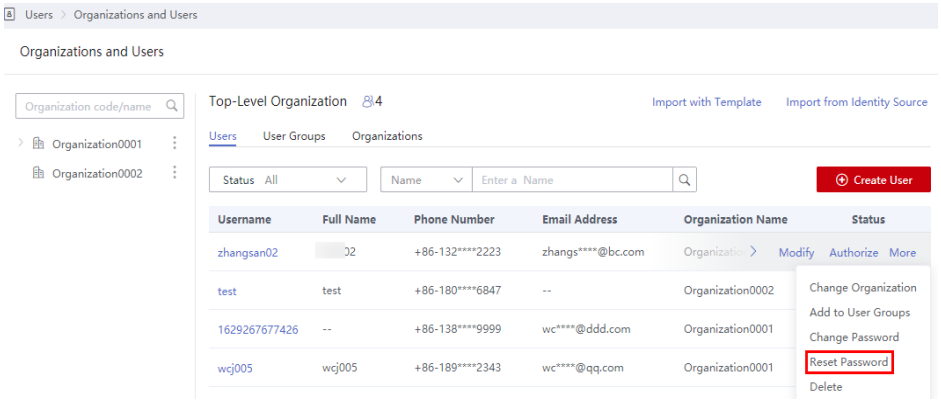
NOTE

- After the password is reset, users must change the password when logging in to the user portal in password mode for the first time.
- To notify users by email, configure the email gateway. For details, see **Email Gateway Configuration**.

Step 1 In the user list, choose **More** > **Reset Password** in the row that contains the target user.

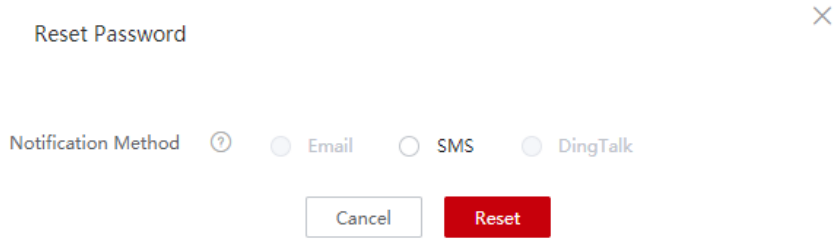
 Copyright © Huawei Technologies Co., Ltd.

Figure 2-15 Resetting the password



Step 2 Select **SMS**.

Figure 2-16 Selecting SMS



Step 3 Click **Reset**. The user can then use the new password to log in to the user portal.

----End

Activating/Deactivating a User

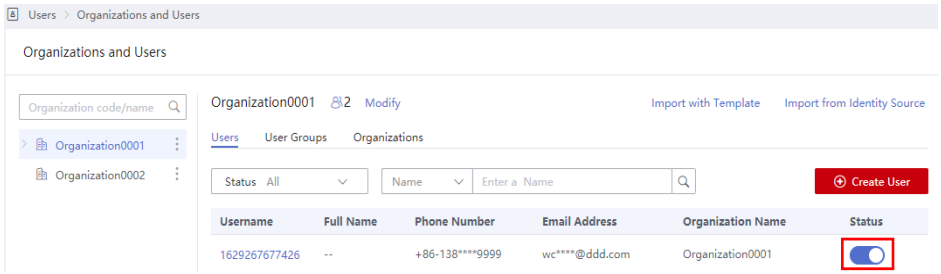
You can activate or deactivate users in the same way. To deactivate a user, do as follows:

CAUTION

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.

Figure 2-17 Deactivating a user



 Copyright © Huawei Technologies Co., Ltd.

Step 2 Click **OK**.

----End

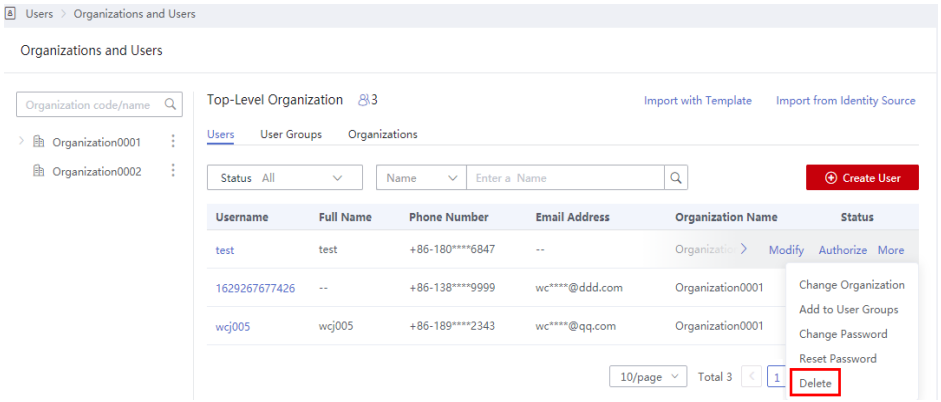
Deleting a User

In the user list, choose **More** > **Delete** in the row that contains the target user and click **OK**.

CAUTION

Deleted users can no longer access the user portal. To add users, see **Creating a User**.

Figure 2-18 Deleting a user



2.2.2 Organizations

Organizations facilitate user management and authorization. You can create, modify, move, and delete organizations, and add users to 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 **Identity Sources**.
- Import with a template: Add organization data to the template and then import the organization data to OneAccess. For details, see **Importing Organizations**.

Adding an Organization

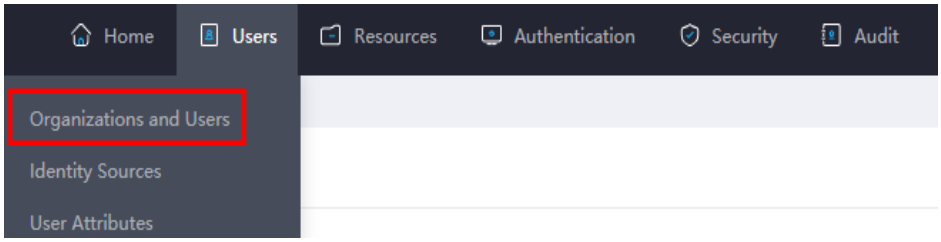
In an organization tree, you can add top-level organizations and sub-organizations.

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Users** > **Organizations and Users**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-19 Organizations and Users



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

Step 4 Click **Create Organization**.

NOTE

- To create a top-level organization, click **+** in the lower left.
- To create a sub-organization, select an organization in the left pane, choose > **Create Sub-organization** (see **Figure 2-21**).

Figure 2-20 Creating an organization

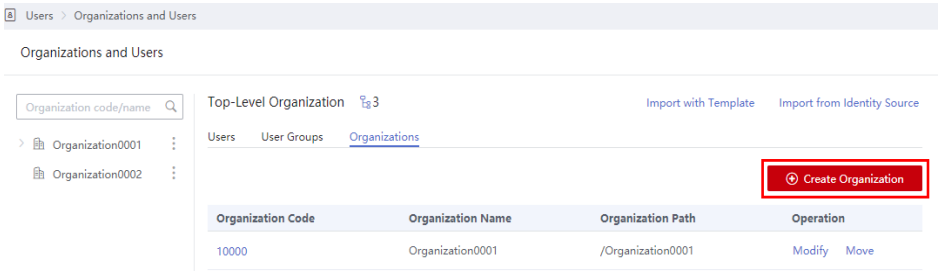
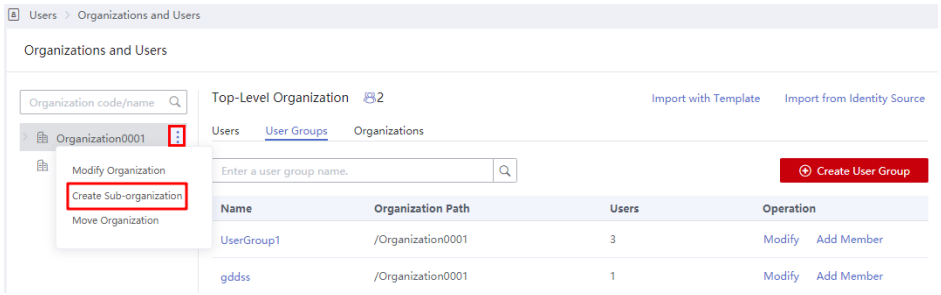


Figure 2-21 Creating a sub-organization



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

Table 2-1 Organization information

Parameter	Description
* Organization Code	Unique identifier of the organization.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
*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	• Displayed as "Top-Level Organization" when you create a top-level organization • Displayed as the organization you selected when you create a sub-organization

Step 6 Click **OK**.

----End

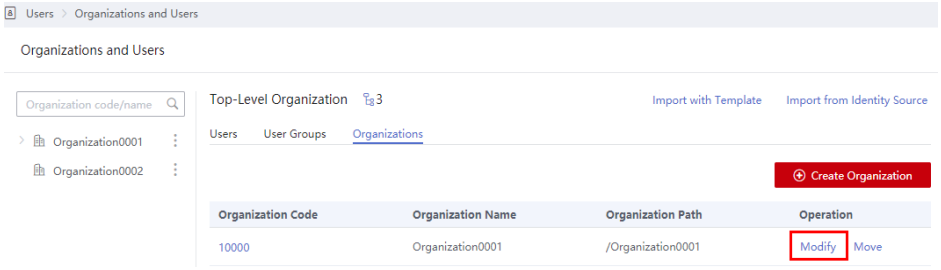
Viewing Organization Details

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. To move an organization to another parent organization, see **Moving an Organization**.

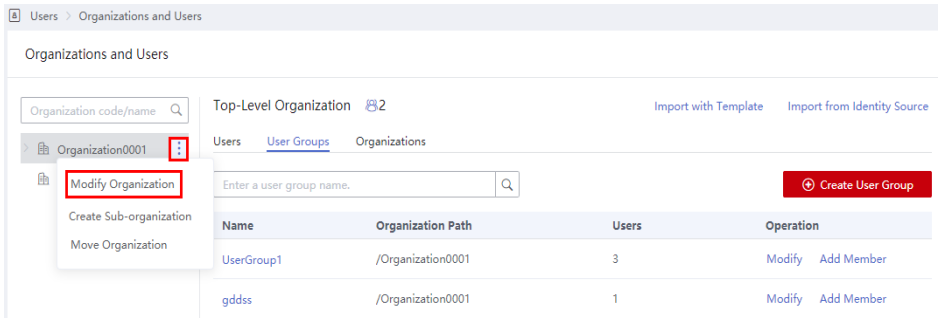
Figure 2-22 Modifying an organization



To modify an organization, select it in the left pane, choose > **Modify Organization** (see **Figure 2-23**).

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-23 Modifying an organization

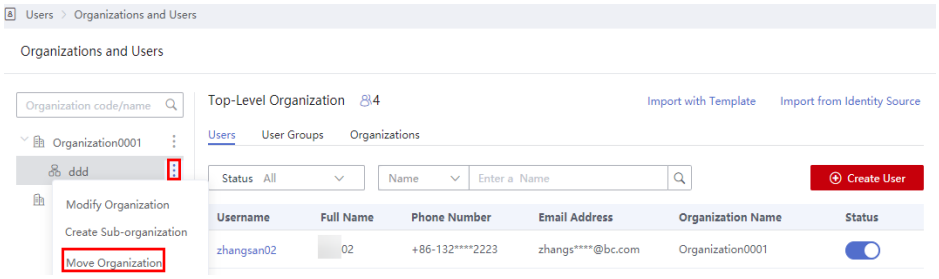


Moving an Organization

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.

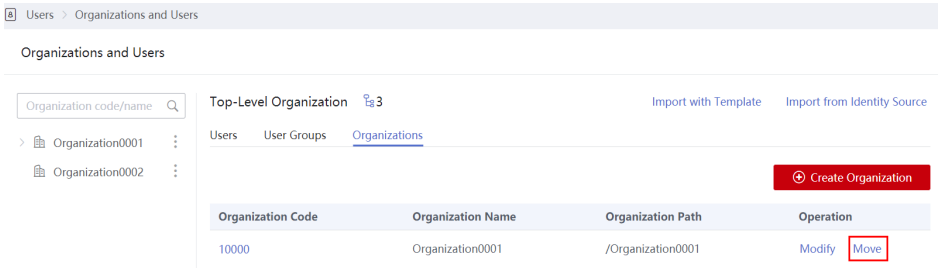
To move an organization, select it in the left pane, choose > **Move Organization** (see **Figure 2-24**).

Figure 2-24 Moving an organization



Step 1 In the organization list, click **Move** in the row that contains the organization you want to move.

Figure 2-25 Moving an organization



Step 2 Select the target parent organization to which you want to move the organization. To set a sub-organization as a top-level organization, click **Set as Root Organization**.

Step 3 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Deleting an Organization

- In the organization list, click **Delete** in the row that contains the organization you want to delete, and click **OK**.
- The organization cannot be recovered once deleted. Exercise caution when performing this operation.
- Delete the users, user groups, and sub-organizations in the organization first.

2.2.3 User Groups

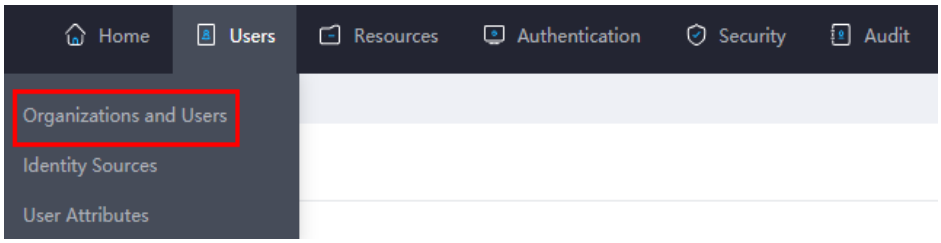
User groups facilitate user management and authorization. You can create, modify, and delete user groups, and add users to them.

Adding a User Group

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Users** > **Organizations and Users**.

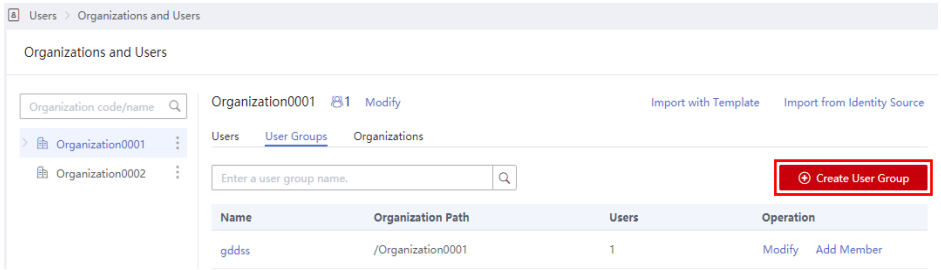
Figure 2-26 Organizations and Users



Step 3 In the left pane, select an organization for which you want to create a user group, and click the **User Groups** tab.

Step 4 Click **Create User Group**.

Figure 2-27 Creating a user group



Step 5 On the **Create User Group** page, enter the user group name and description.

Step 6 Click **OK**.

----End

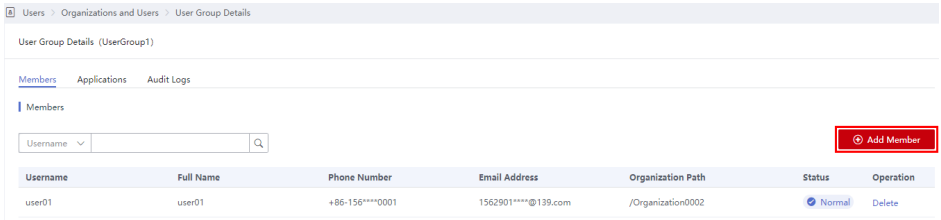
Viewing User Group Details

In the user group list, click a user group to view its **members**, **applications**, and **audit logs**.

 Copyright © Huawei Technologies Co., Ltd.

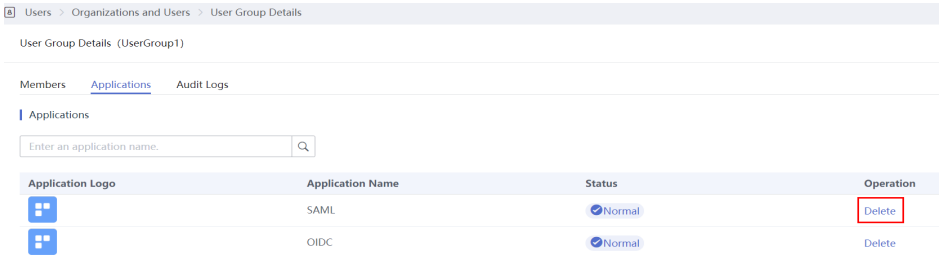
- Members
  - Users in the user group, including the username, mobile number, and email address.
  - To add more users to the user group, click **Add Member** in the upper right. For details, see **Adding Users to a User Group**.

    Figure 2-28 Adding members

  - To remove a user from the user group, click **Delete** in the **Operation** column of the row that contains the user.
- Applications
  - 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 not be synchronized to the application.

    Figure 2-29 Canceling authorization for an application

- Audit Logs

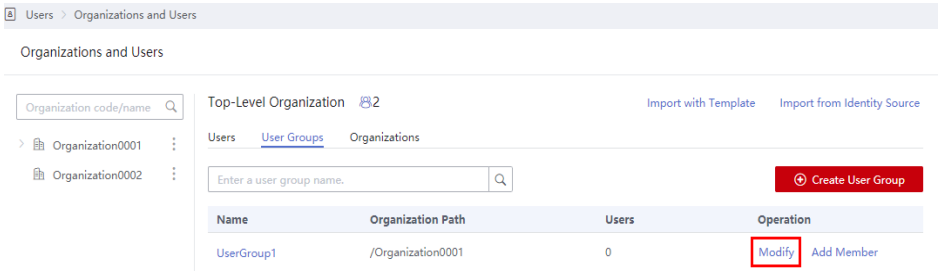
  Administrators' operations on the user group, such as group creation and member addition. Set filter conditions to view desired logs.

Modifying User Group Information

Click **Modify** in the row that contains the target user group, and modify its name and description. The organization to which the user group belongs cannot be changed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-30 Modifying a user group

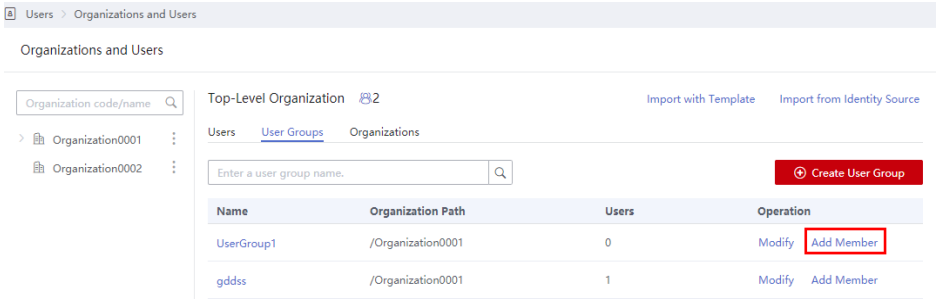


Adding Users to a User Group

Add members of different organizations to a user group for easy management and authorization.

Step 1 In the user group list, click **Add Member** in the row that contains the user group.

Figure 2-31 Adding members



Step 2 On the **Add Member** page, select the users you want to add, and click **Save**.

----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 contained in the user group.

2.2.4 Identity Sources

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 WeChat, DingTalk, Active Directory (AD), and Lightweight Directory Access Protocol (LDAP). With only simple configuration, you can

 Copyright © Huawei Technologies Co., Ltd.

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 can integrate user and organization information of different identity sources, such as WeCom, DingTalk, AD, and LDAP. Configuration information varies depending on the identity source. See the following links:

- **Integrating AD**
- **Integration LDAP**

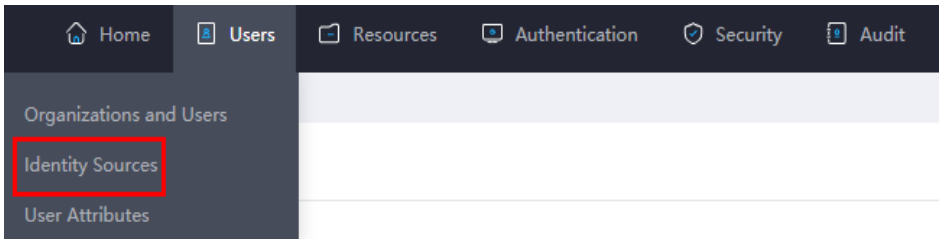
This section describes how to add an identity source. DingTalk is used for illustration.

Procedure

Step 1 Add an identity source.

1. In the top navigation pane, choose **Users** > **Identity Sources**.

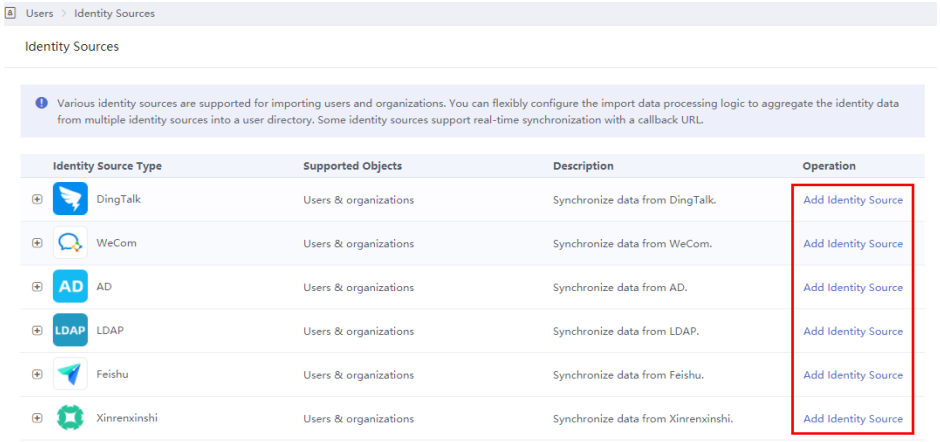
   Figure 2-32 Identity Sources

2. On the **Identity Sources** page, click **Add Identity Source** in the row that contains the identity source type you want to add.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-33 Adding an identity source

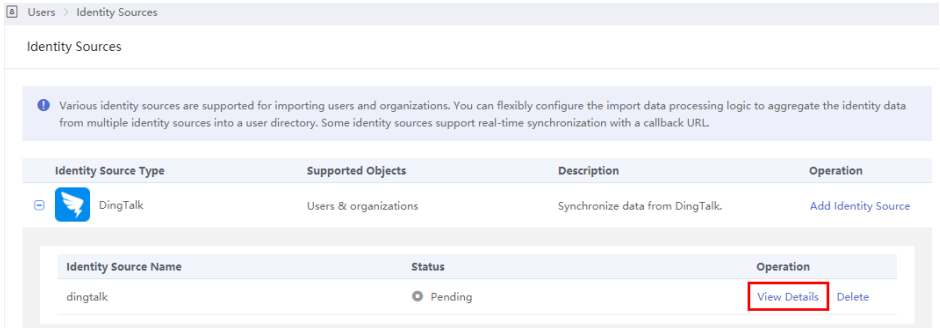


3. Enter an identity source name and click **OK**.

Step 2 Configure the import settings.

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

Figure 2-34 Clicking View Details



2. Click the **Import Settings** tab.
3. Set the import parameters and click **Save**.

Table 2-2 Configuration parameters

Parameter		Description
Import Settings	Enterprise ID	(Required) Enterprise ID on the identity source open platform, for example, **CorpId** on DingTalk.
	AppKey	(Required) Key of an application created on the identity source open platform. For example, in DingTalk, **AppKey** indicates the application key.
	AppSecret	(Required) Secret of the application. For example, in DingTalk, **AppSecret** indicates the application secret.

 Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	Root Department ID	(Required) ID of the department from which you want to synchronize user data. The default value is **1**, indicating that user data of all organizations in the identity source will be synchronized to OneAccess. To synchronize user data from a specific department, enter the ID of the department.
	Proxy Server Address	(Optional) IP address or domain name of your server that you want to use to synchronize data from the identity source in real time.
	Callback	Disabled by default, indicating that OneAccess will not synchronize data from the identity source in real time.
	Callback URL	Automatically generated after you enable callback.
	Event Type	Automatically generated after you enable callback.
Advanced Settings (Optional)	Organization	Organization in OneAccess to which data from the identity source will be synchronized. If no organization is selected, a new root organization will be created in OneAccess.
	Deletion Threshold	Number of data records deleted in the identity source that will trigger data protection in OneAccess. For example, if the number of data records deleted in the identity source exceeds the specified limit, the same data will remain in OneAccess.
	Organization Matching	Organization mapping rules for OneAccess to synchronize organization data from the identity source. For example, if you add a rule with the OneAccess attribute **code** and the identity source attribute **organization code**, organization data synchronized from the identity source will be identified using their **organization code**.
	Create Organization	Enabled by default, indicating that OneAccess will automatically create new organizations for those that do not match any existing organizations in OneAccess. You are advised to keep this option enabled.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	Update Organization	Enabled by default, indicating that the organizations in OneAccess that match those synchronized from the identity source will be updated. You are advised to keep this option enabled.
	Delete Organization	Indicates whether to delete the organizations in OneAccess if the same organizations are deleted in the identity source.
	User Matching	User mapping rules for OneAccess to synchronize user data from DingTalk.
	Create User	By default, this option is enabled, indicating that users noting match any existing users in OneAccess will be created.
	Update User	By default, this option is enabled, indicating that the users in OneAccess that match those synchronized from the identity source will be updated.
	Delete User	Indicates how to handle the users in OneAccess if they are deleted in the identity source. You can disable or retain the users.

Step 3 Click the **Object Models** tab, set user and organization attributes and mapping rules.

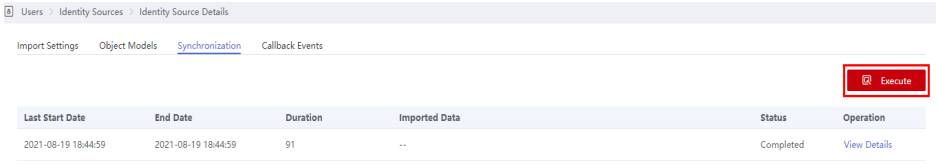
Table 2-3 Object model

Parameter		Description
User Object	Attributes	User attributes (for example, userid) to be synchronized from the identity source to OneAccess.
	Mappings	Data conversion rules for synchronizing user data from the identity source to OneAccess. Script-based conversion is supported.
Organization Object	Attributes	Organization attributes (for example, code) to be synchronized from the identity source to OneAccess.
	Mappings	Data conversion rules for synchronizing organization data from the identity source to OneAccess. Script-based conversion is supported.

Step 4 Click the **Synchronization** tab, and click **Execute** to synchronize data from the identity source.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-35 Clicking Execute



Step 5 Click the **Callback Events** tab, and view the interactions between OneAccess and the identity source, including creating, updating, and deleting data.

----End

2.2.5 User Attributes

To synchronize more user information to downstream applications, add user attributes.

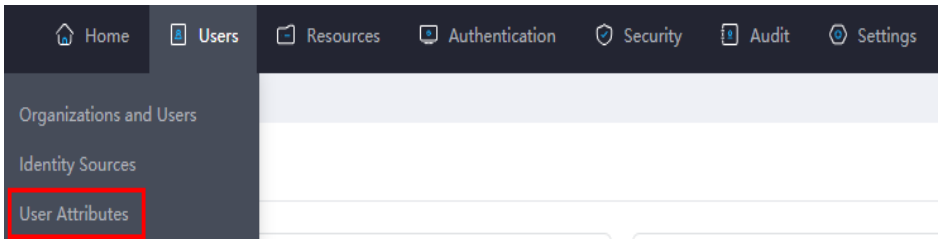
- Basic attributes: preset user attributes, such as username and mobile number. Basic attributes can be modified but cannot be created or deleted.
- Extended attributes: Preset extended attributes can be modified and deleted. You can also add more attributes, such as length of service and employee level.

Adding an Extended Attribute

Step 1 Log in to the administrator portal.

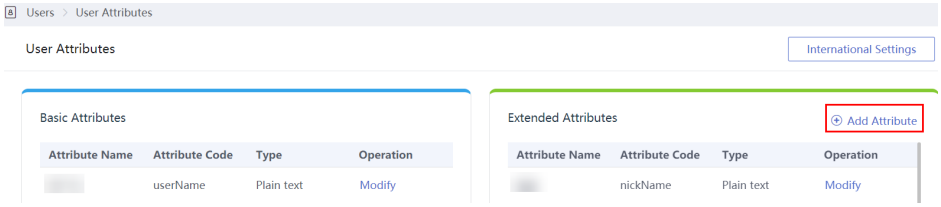
Step 2 In the top navigation pane, choose **Users** > **User Attributes**.

Figure 2-36 User Attributes



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

Figure 2-37 Adding an attribute



Step 4 Enter the attribute information.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-4 Basic settings

Parameter	Description
* Attribute Name	The attribute name must be unique.
* Attribute Code	The attribute code must be unique.
* Type	• **Options** vary depending on the attribute type. • If you set **Type** to **Dictionary**, select a dictionary. For details about how to add a dictionary, see **Dictionaries**. • If you set **Type** to **Sensitive text**, the attribute will be partially anonymized by default.
Default Value	Default value of the user attribute. This parameter is available only if you set **Type** to **Plain text**, **Number**, or **Switch**.
Description	Description of the attribute.
Options	The options vary depending on the **attribute type**.
* Associated Dictionary	If you set **Type** to **Dictionary**, select a dictionary by referring to **Dictionaries**.

Table 2-5 Display settings

Parameter		Description
Sequence		• Specify the position of an attribute in the extended attribute list. By default, a new attribute is displayed in the top of the list. • The attribute will be displayed in the specified position on the user creation page.
Administrator or Portal	Display in query conditions	Indicates whether to display the attribute in the user query conditions.
	Display in query result list	Indicates whether to display the attribute in the user list. For example, if you select this option for the basic attribute **email**, the email address of each user will be displayed in the user list.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	Create User	• **Read/Write**: The attribute will be displayed and can be modified when you add a user. • **Read-only**: The attribute will be displayed but cannot be modified when you add a user. • **Hide**: The attribute will not be displayed when you add a user.
	Query/Modify User	• **Read/Write**: The attribute will be displayed and can be modified when you modify a user. • **Read-only**: The attribute will be displayed but cannot be modified when you modify a user. • **Hide**: The attribute will not be displayed when you modify a user.
User Portal	Personal Information Page	• **Read/Write**: The attribute will be displayed and can be modified when a user views their personal information. • **Read-only**: The attribute will be displayed but cannot be modified when a user views their personal information. • **Hide**: The attribute will not be displayed when a user views their personal information.
	Registration Page	• **Read/Write**: The attribute will be displayed and can be modified when a user registers an account. • **Read-only**: The attribute will be displayed but cannot be modified when a user registers an account. • **Hide**: The attribute will not be displayed when a user registers an account.

Step 5 Click **Save**.

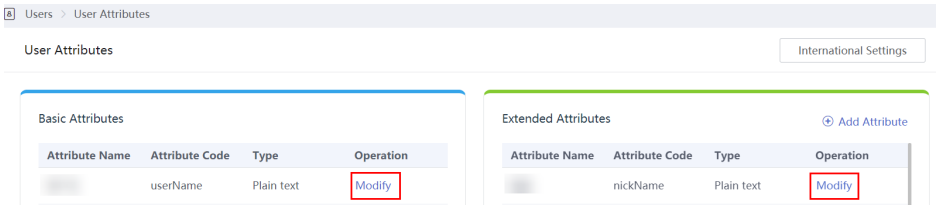
----End

Modifying a Basic or Extended Attribute

On the **User Attributes** page, click **Modify** in the **Operation** column of the row that contains the basic or extended attribute you want to modify, and then modify the basic information and display settings of the attribute. The attribute code and type cannot be modified.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-38 Modifying an attribute



Deleting an Extended Attribute

On the **User Attributes** page, click **Delete** in the **Operation** column of the row that contains the extended attribute you want to delete, and click **OK**.

NOTE

- Basic attributes cannot be deleted.
- Deleted extended attributes cannot be recovered. Exercise caution when performing this operation.

2.3 Resources

2.3.1 Overview

Centrally manage applications, enterprise APIs, and enterprise devices. This chapter describes how to do this with OneAccess.

Applications

Applications are downstream systems of your enterprise. After you configure applications, users can access them from OneAccess through single sign-on (SSO).

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

To manage applications and authorize access, see the following sections:

Adding an Application

Configuring an Application

Enabling or Disabling an Application

Deleting an Application

Enterprise APIs

OneAccess supports system and custom APIs.

- System APIs

  A group of built-in APIs for accessing OneAccess.
- Custom APIs

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

 Copyright © Huawei Technologies Co., Ltd.

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.

To manage and authorize API access, see the following sections:

Authorizing Access to Built-in APIs

Calling Built-in APIs

Modifying Built-in APIs

Adding a Custom API

Configuring a Custom API

Deleting a Custom API

Enterprise Devices

OneAccess provides the RADIUS server and supports authentication using VPNs provided by Huawei, Sangfor, H3C, and other vendors. You can manage these VPNs in the administrator portal.

To manage enterprise devices, see the following sections:

Adding an Enterprise Device

Modifying Device Information

Deleting an Enterprise Device

2.3.2 Adding an Application

Add custom or pre-integrated downstream applications.

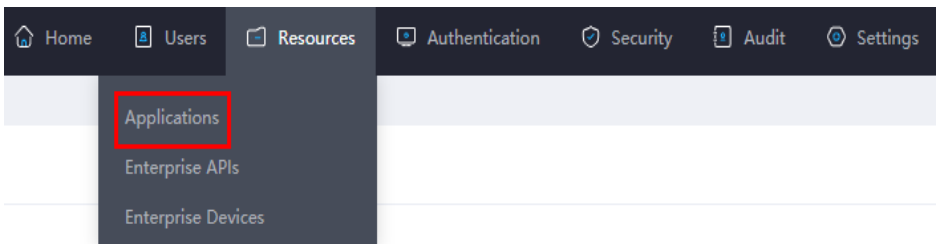
Adding a Custom Application

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 In the top navigation pane, choose **Resources** > **Applications**.

Figure 2-39 Applications



Step 3 On the **Applications** page, click **Add Custom Application**.

Copyright © Huawei Technologies Co., Ltd.

Step 4 Enter an application name, and click **Save**.

Step 5 Configure the parameters required so that the application can be accessed by users. For details, see **Configuring an Application**.

----End

Adding a Pre-integrated Application

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

Step 1 On the **Applications** page, click **Add Pre-integrated Application**.

Step 2 Click the pre-integrated application you want to add.

Step 3 Enter an application name, and click **Next**.

Step 4 Set the authentication parameters. The authentication method and parameters vary depending on the application. SAML is used for illustration. For details about how to add HUAWEI CLOUD, see **SSO Access to HUAWEI CLOUD**.

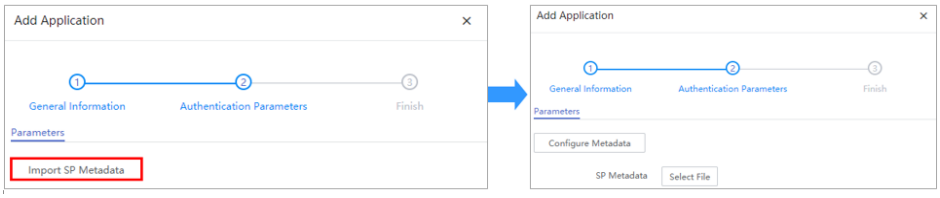
To add an application through SAML, upload a metadata file or edit the metadata manually.

- 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.

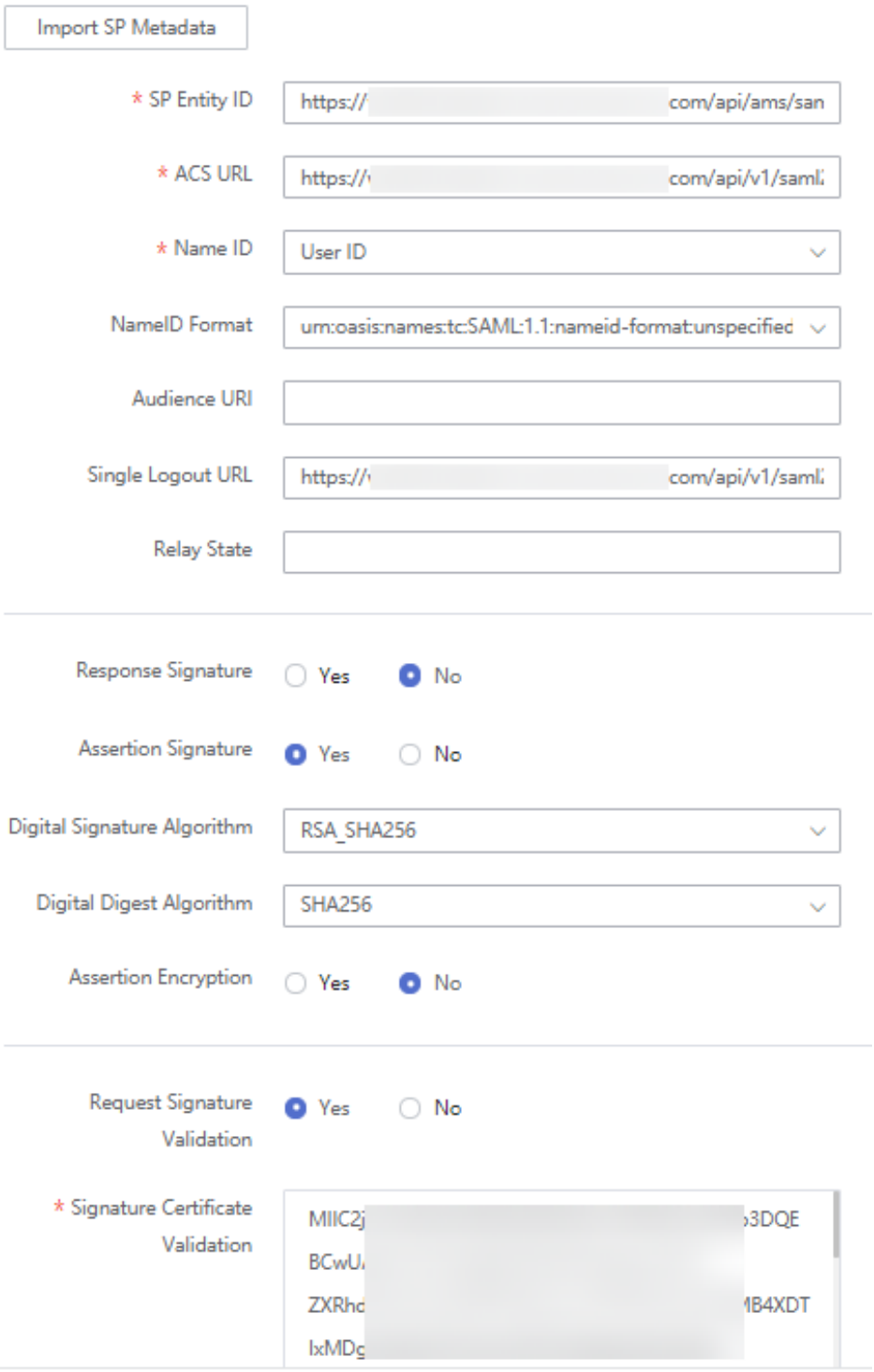
  Figure 2-40 Uploading a metadata file

  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.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-41 Editing metadata



 Copyright © Huawei Technologies Co., Ltd.

Table 2-6 Authentication parameters

Parameter	Mandatory	Description
SP Entity ID	Yes	Unique identifier of an SP. Enter the value of **Entity ID** displayed in the SP metadata file.
ACS URL	Yes	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	Yes	Select a user attribute or account attribute. The attribute value will be used as the subject of the assertion.
NameID Format	Yes	Username format supported by the SP. Enter the value of **NameIDFormat** displayed in the SP metadata file.
Audience URI	No	Audience for which the SAML assertion is intended. By default, this field is the same as **SP Entity ID**.
Single Logout URL	No	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.
Default Relay State	No	Default URL to which users will be redirected after successful login.
Response Signature	Yes	Indicates whether to sign SAML responses using the identity provider's (IdP) certificate. By default, SAML responses are not signed.
Assertion Signature	Yes	Indicates whether to sign assertions using the IdP's certificate. By default, assertions are not signed. Enter the value of **WantAssertionsSigned** displayed in the SP metadata file.
Digital Signature Algorithm	Yes	Algorithm used to sign SAML responses or assertions. By default, **RSA_SHA256** is used. The options include **RSA_SHA256**, **RSA_SHA512**, and **RSA_RIPEMD160**.
Digital Digest Algorithm	Yes	Algorithm used to create digests for SAML responses or assertions. By default, **SHA256** is used. The options include **SHA256**, **SHA512**, and **RIPEMD160**.
Assertion Encryption	Yes	Indicates whether to encrypt assertions. By default, assertions are not encrypted.
Request Signature Validation	Yes	Indicates whether to sign SAML requests. By default, SAML requests are signed. Enter the value of **AuthnRequestsSigned** displayed in the SP metadata file.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
Signature Certificate Validation	Yes	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 5 (Optional) If the application supports data synchronization, set the synchronization parameters. You can then manage accounts and groups of the application in OneAccess. The synchronization method and authentication parameters vary depending on the application. OneAccess can synchronize data through event callback, System for Cross-domain Identity Management (SCIM), or Lightweight Directory Access Protocol (LDAP). This step uses SCIM for illustration. For details, see **Synchronizing Data with Atlassian Through SCIM**.

Table 2-7 Synchronization parameters

Parameter		Description
Basic Settings	SCIM Endpoint	Address of the target system to receive SCIM data.
	Authentication Method	Authorization is required for calling SCIM APIs. The options include **Basic Auth** and **Bearer Token**.
	Username	Username corresponding to the specified authentication method.
	Password	Password corresponding to the specified authentication method.
	Application Account Template	User data template to be pushed to the target system. Fill attributes as required. OneAccess provides a data template that complies with SCIM 2.0.
	Application Organization Template	Organization data template to be pushed to the target system. Fill attributes as required. OneAccess provides a data template that complies with SCIM 2.0.
	Organization Resource Path	Organization resource path in SCIM. For example, the user path is **User** and the user group path is **Group**.
Advanced Settings	Content-Type	Request header parameter, which you can set based on the target system. Set this parameter to **application/json** or **application/scim+json**. The default value is **application/scim+json**.
	Accept	Request header parameter, which you can set based on the target system. Set this parameter to **application/json** or **application/scim+json**.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	Time Format	JSON time format. If the time is in milliseconds, set this parameter to **timestamp**. If the time is another type of value, enter an expression, for example, **yyyy-MM-dd HH:mm:ss**.

Step 6 Click **Save**. Go to the application details page, and modify the settings by referring to **Configuring an Application**.

----End

2.3.3 Configuring an Application

Configurations of an application include the general information, authentication settings, synchronization settings, login settings, access control, object models, authorization, API permissions, and application permissions. Perform the following procedure to configure custom or pre-integrated applications.

Step 1 On the **Applications** page, click the application you want to configure.

Step 2 Click the application logo or name to go to the application details page.

Step 3 Modify the general information.

Figure 2-42 Modifying general information

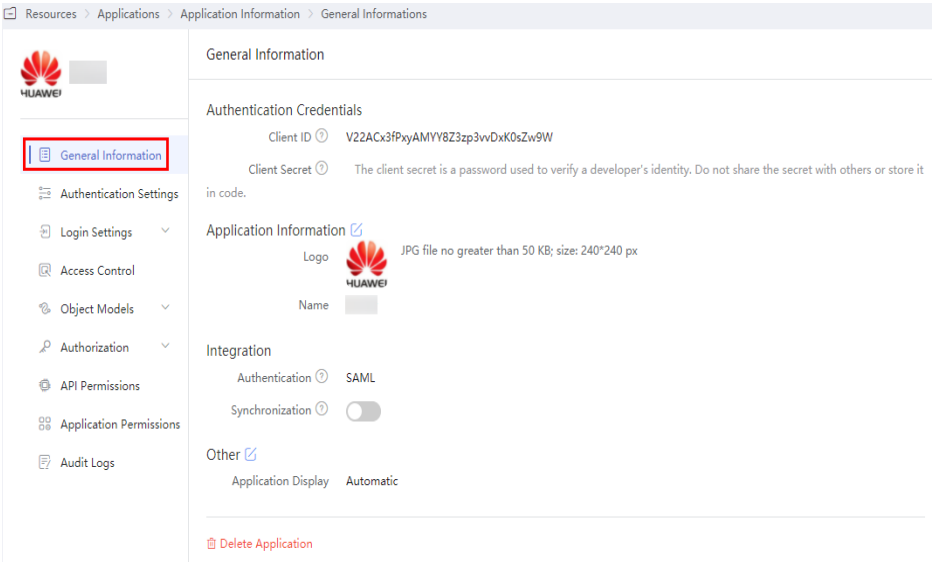


Table 2-8 General information

Application Information		Description
Authentication Credentials	Client ID	API authentication ID. It is automatically generated by OneAccess.

Copyright © Huawei Technologies Co., Ltd.

Application Information		Description
	ClientSecret	API authentication secret. To obtain the secret, click **Enable**. **NOTE** • The secret has unlimited validity. Keep it secure. • To obtain a new secret, click **Reset**. • After you reset the secret, it becomes invalid and the new secret takes effect immediately.
Application Information	Logo	(Optional) Upload a JPG file whose size is no greater than 50 KB. 240 x 240 pixels is recommended.
	Name	(Required) Name of the application.
Integration	Authentication	Protocol for integrating the application with OneAccess for identity authentication. OAuth, SAML, OIDC, CAS, and plug-in autocompletion are supported. **NOTE** The protocol cannot be changed once specified.
	Synchronization	Method of synchronizing data between the application and OneAccess. Event callback, SCIM, and LDAP are supported. **NOTE** The synchronization mode cannot be changed once specified.
Other	Application Display	Display mode of the application in the user portal. • **Automatic**: The application is displayed on the homepage of the user portal only for users who have access to the application. • **Fixed**: The application is displayed on the homepage of the user portal for all users. • **Not display**: The application is not displayed on the homepage of the user portal for any users.

Step 4 (Optional) If you have specified an authentication protocol in **Step 3**, modify the authentication parameters and mappings.

- **Parameters**: Modify the authentication parameters of the application by referring to **Step 4**.
- **Mappings**: Configure mappings between OneAccess and the application for user attributes, real-name attributes, account attributes, account permissions, social attributes, fixed attribute values, and dynamic scripts. For details, see *Best Practices*.

Step 5 (Optional) If you have specified a synchronization method in **Step 3**, modify the synchronization parameters and configure the method of handling account and organization data.

 Copyright © Huawei Technologies Co., Ltd.

- **Parameters**: Modify the synchronization parameters of the application by referring to **Step 5**.
- **General**: Configure whether to synchronize deleted accounts and organizations and deactivated accounts from OneAccess to the application.

Step 6 Modify the login configuration. OneAccess allows you to configure PC- and mobile-based login authentication methods for each application.

- **Web Applications**: Users use a specific URL to access the application on a PC.

  You can enable multiple authentication methods for PC-based access to the application. For details, see *Best Practices*.
- **Mobile Applications**: Users use a specific URL to access the application on a mobile device.

  You can enable multiple authentication methods for mobile device–based access to the application. For details, see *Best Practices*.
- **Official Accounts**: Users use a WeChat official account to access the application in password-free mode.

NOTE

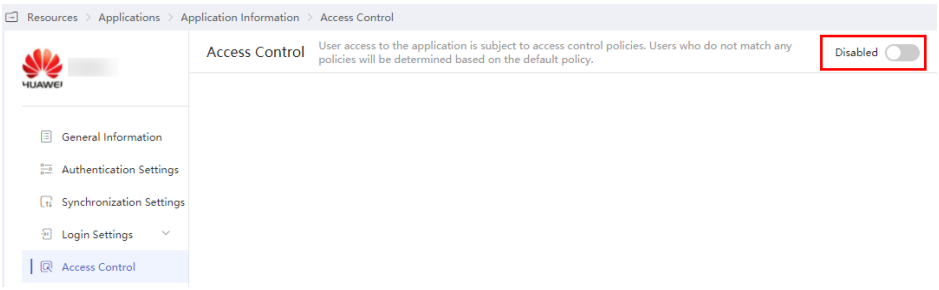
Before enabling an authentication method, ensure that you have configured the corresponding authentication provider. For details, see **Adding an Authentication Provider**.

Step 7 Modify the access control settings. When enabling access control, set the default access control policy. Then you can create custom policies.

- Default policy: If no custom policies are matched, the default policy is used to determine whether users can access the application. The default policy **cannot** be deleted or disabled.

  a. On the **Access Control** page, enable access control.

  Figure 2-43 Enabling access control



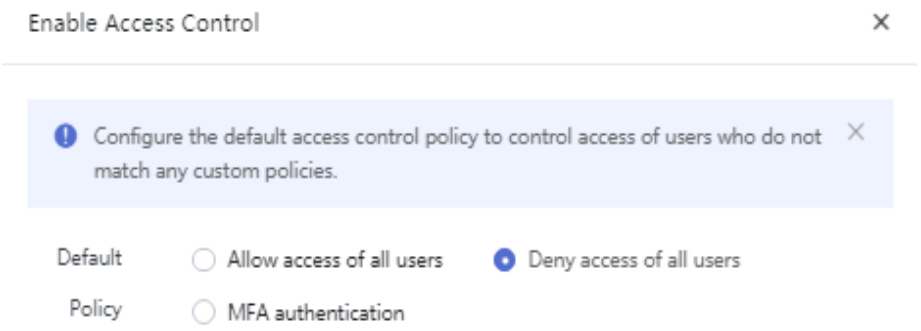
  b. On the **Enable Access Control** page, configure the default policy.

NOTE

To ensure application security, select **Deny access of all users**.

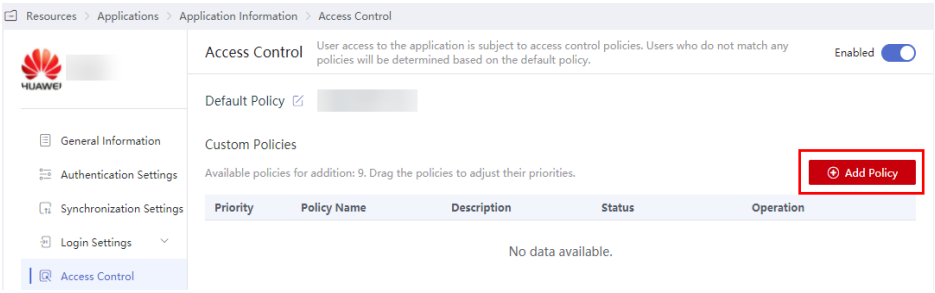
Copyright © Huawei Technologies Co., Ltd.

Figure 2-44 Configuring the default policy



- Add, modify, view, delete, enable, and disable access control policies for the application.
  a. On the **Access Control** page, click **Add Policy**.

  Figure 2-45 Adding a policy

  b. On the **Add Access Control Policy** page, set the policy information and click **Save**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-46 Add an access control policy

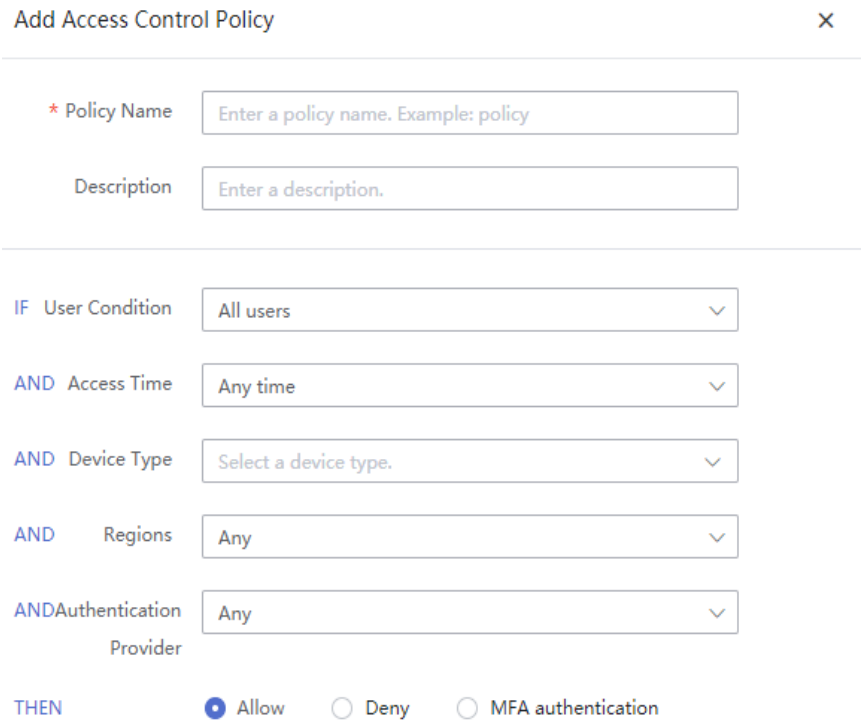


Table 2-9 Policy information

Parameter	Description
Policy Name	(Required) Name of the access control policy.
Description	(Optional) Description about the access control policy.
User Condition	(Required) Range of users who are allowed or not allowed to access the application. The options include **All users**, **Qualified users**, and **Disqualified users**. To control access of specific users, set the user conditions described in **Table 2-10**.
Access Time	(Required) 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**. To control access in specific time range, set the date and time.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Device Type	(Optional) Type of devices that are allowed or not allowed to access the application. The options include **Browser**, **Desktop device**, and **Mobile device**. ■ Browser: Google Chrome, Firefox, Internet Explorer, and other ■ Desktop device: Windows, Linux, macOS, and other ■ Mobile device: Android, iOS, and other
Regions	(Required) Countries or regions where users are allowed or not allowed to access the application. The options include **Any**, **Chinese Mainland**, **Outside the Chinese Mainland**, **Within specific regions**, and **Outside specific regions**. This field is required. To specify a region, select **Within specific regions** and select a region (IP address range). If no regions are available, create one by referring to **Regions**.
Authentication Provider	(Required) 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**. If you select **With specific authentication providers**, specify an authentication provider.
THEN	(Required) Allow or disallow users who meet the conditions to access the application, or require the users to perform verification. If you select **MFA authentication**, set the following parameters: ■ **Frequency**: Require users to perform verification during login or for every session. ■ **Authentication Method**: Require users to perform verification through one-time password (OTP) or SMS. For details about how to configure OTP, see **OTP**.

Table 2-10 User conditions

Parameter	Description
Condition Type	(Required) Options: **or**, **and**
User Group	Group of users who are allowed or disallowed to access the application. For details, see **User Groups**.

Copyright © Huawei Technologies Co., Ltd.

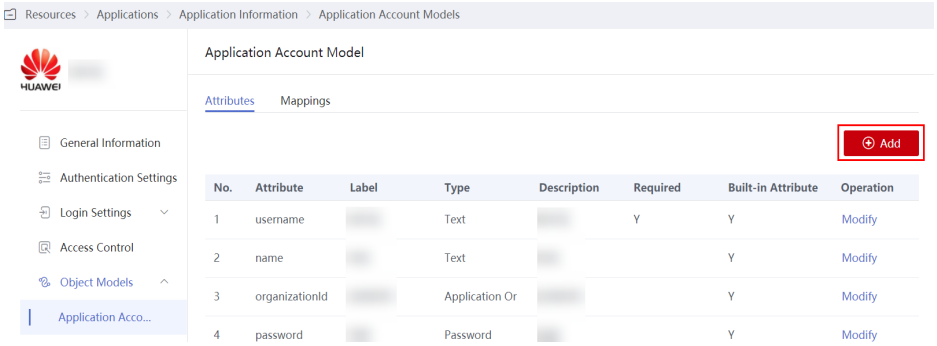
Parameter	Description
Organization	Organization of users who are allowed or disallowed to access the application. For details, see **Organizations**.
Users	Users who are allowed or disallowed to access the application. For details about users, see **Users**.
Custom Condition	Define custom conditions based on user attributes. For details about user attributes, see **User Attributes**. **NOTE** To add more custom conditions, click **Add Custom Condition**. Select at least one user condition.

Step 8 Modify the object models, including the application account model and application organization model. They are the basis for synchronizing users and organizations from OneAccess to the application.

- Attributes

  Customize account and organization attributes for the application. Built-in attributes can only be modified and cannot be deleted. To use more attributes, click **Add** to add custom attributes. Custom attributes can be modified and deleted.

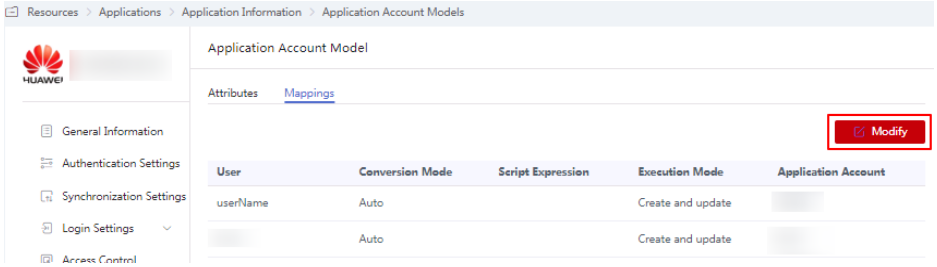
  Figure 2-47 Adding an attribute



- Mappings

  To synchronize users and organizations from OneAccess to the application, establish mappings between them.

  Figure 2-48 Modifying mappings

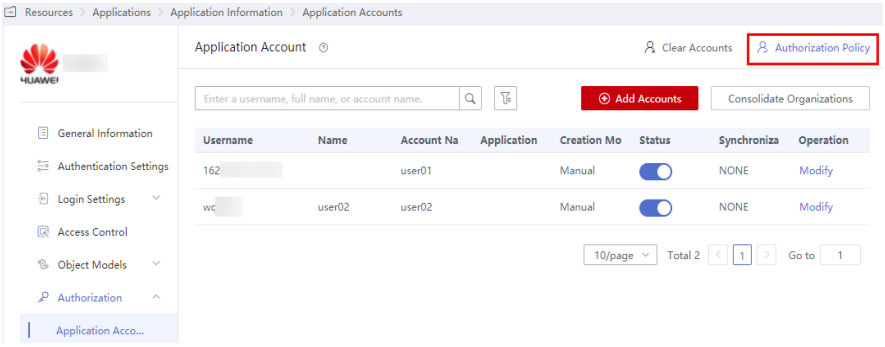


Step 9 Authorize access to users and organizations, view synchronization events, and manage orphan accounts and shared accounts.

Copyright © Huawei Technologies Co., Ltd.

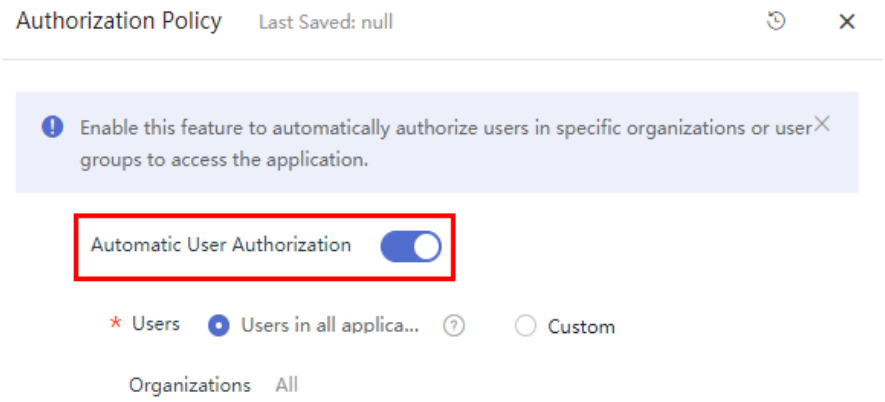
- Application accounts: Manage the mappings between **OneAccess users** and **application accounts**. You can map a OneAccess user to accounts of different applications.
  - Authorization policy: Configure automatic authorization for all or specific users in synchronized organizations.
    i. On the **Application Accounts** page, click **Authorization Policy**.

Figure 2-49 Configuring the authorization policy



ii. Enable automatic user authorization.

Figure 2-50 Enabling automatic user authorization



iii. Select users.

Table 2-11 User selection

Parameter	Description
Users in all application organizations	Authorize access to all users in synchronized organizations. If no organizations have been synchronized, all users in OneAccess are authorized.
Custom	Authorize access to users in specific organizations or user groups. If no organizations have been synchronized, users in all organizations are authorized.

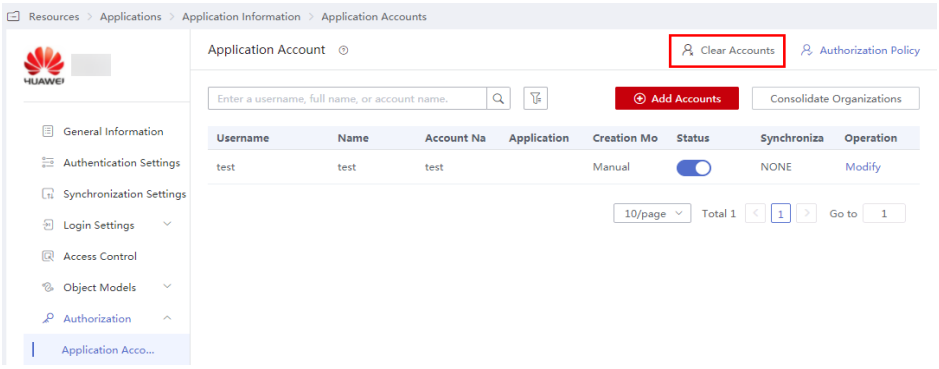
 Copyright © Huawei Technologies Co., Ltd.

iv. (Optional) Click **Save** to save the policy without synchronizing users immediately.

v. Click **Add**. Users are synchronized and displayed in the application account list.

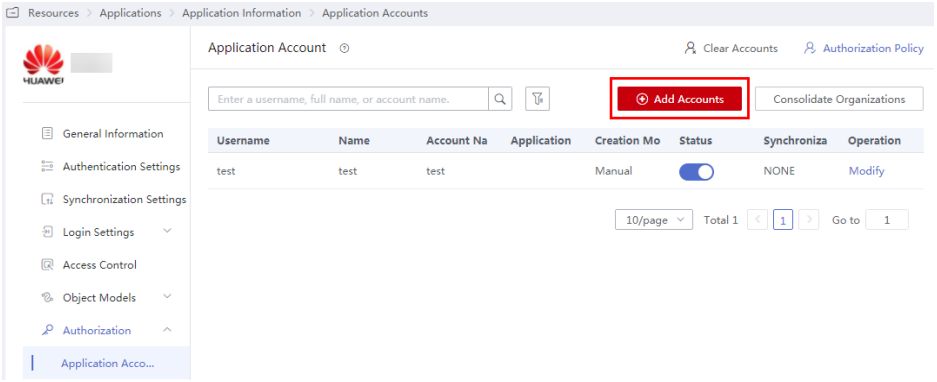
- Clearing accounts: Clear the account data of the application. The operation cannot be undone. Exercise caution when performing this operation.

Figure 2-51 Clearing accounts



- Adding accounts: Manually authorize access to specific users and set application accounts for them.

Figure 2-52 Adding accounts



- Organization consolidation: The system automatically consolidates users' organizations.

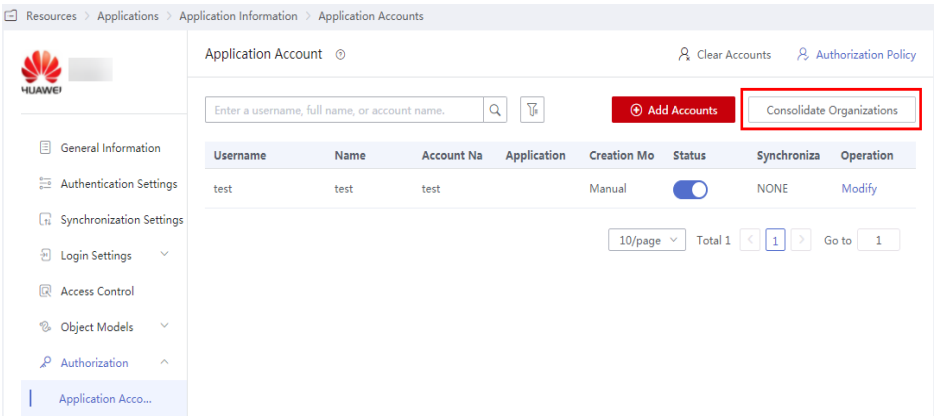
  This feature is available only for certain applications. Skip this step if your application does not support it.

  NOTE

  Enable the application organization model before consolidating organizations.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-53 Consolidating user organizations

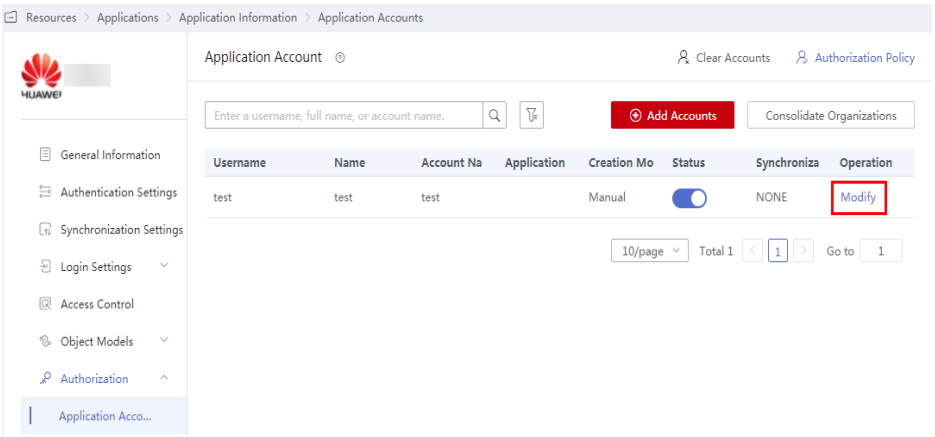


- Modifying accounts: To modify the information about an application account, click **Modify** in the row that contains the account.

  NOTE

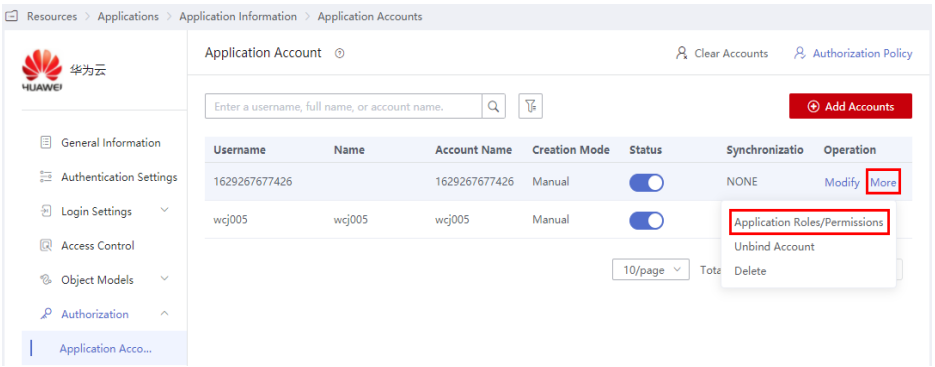
  You can also customize the account information by setting attributes. For details, see **Attributes**.

Figure 2-54 Modifying an account



- Application roles and permissions: Choose **More** > **Application Roles/Permissions** in the row that contains the target application account to assign roles and permissions. For details, see **Step 11**.

Figure 2-55 Application Roles and Permissions



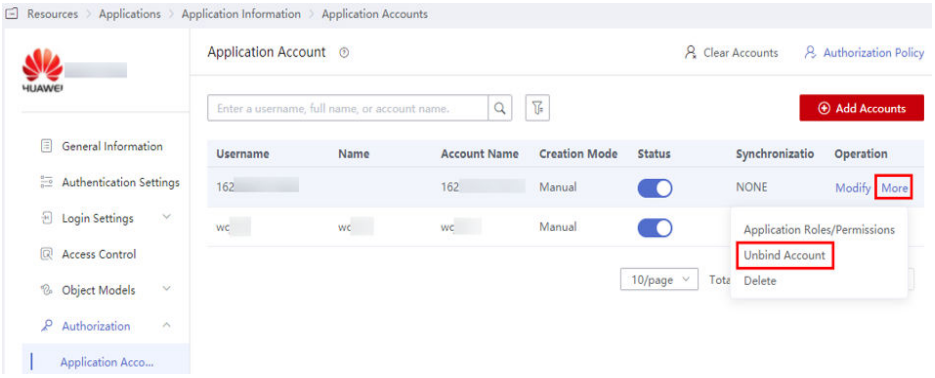
 Copyright © Huawei Technologies Co., Ltd.

- Unbinding accounts: Choose **More** > **Unbind Account** in the row that contains the target application account, and click **OK**.

  NOTE

  Once unbound, application accounts become orphan accounts. You can bind them again to users. For details about orphan accounts, see **Orphan accounts**.

  Figure 2-56 Unbinding an account

- Deleting accounts: To delete an application account, choose **More** > **Delete** in the row that contains the account, and click **OK**.

- Synchronization events: Records of data synchronization between OneAccess and the application. You can filter synchronization events by date range, object type, and object name, and view details of each event. If synchronization failed, view the response and resolve the issue, and then try again.
- Orphan accounts: Application accounts that are created or imported to OneAccess but have not been associated with any OneAccess users. You can edit and delete orphan accounts, associate them with users, and convert them into shared accounts.
- Shared accounts: Application accounts that are shared by multiple OneAccess users. You can add, edit, and delete shared accounts, and specify a controller and users.
  - The controller authorizes and cancels access of users to the application in the administrator portal.
  - Users access the application through the user portal.

Step 10 Manage and view the enterprise APIs that the application can access.

Step 11 Modify application permissions. You can manage application permissions only by roles or by roles, permissions, and resources.

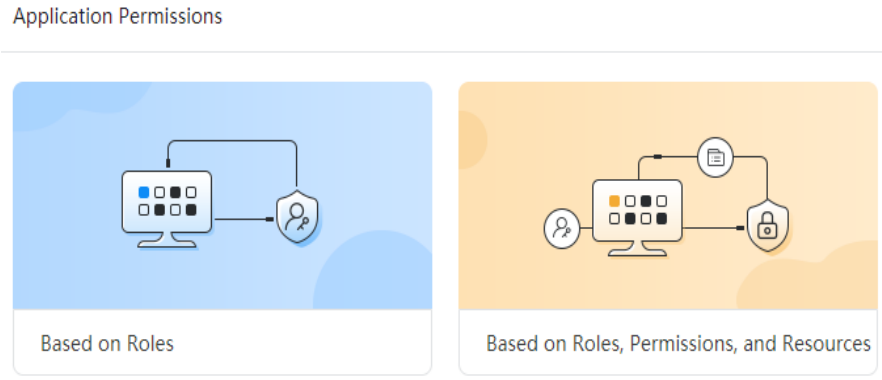
- Permissions management by roles: A type of coarse-grained authorization mechanism that allows you to manage permissions based on user responsibilities. Users with different responsibilities are granted the corresponding roles. Roles and permissions are managed by the application.

  a. On the application details page, choose **Application Permissions**.

  b. On the **Application Permissions** page, click **Based on Roles**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-57 Permissions management by roles



c. On the **Based on Roles** page, enter a role name and role code, and click **Save**. A role is created and displayed on the **Application Permissions** page.

Figure 2-58 Adding a role



Table 2-12 Role information

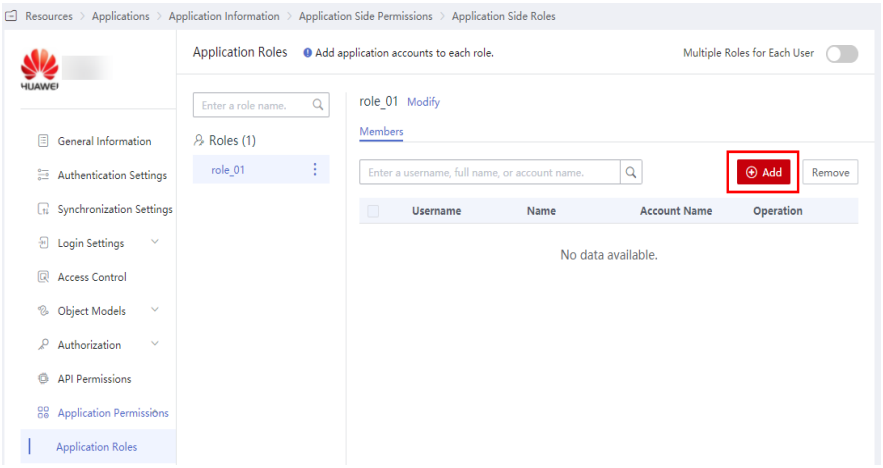
Parameter	Description
* Role Name	Name of the role.
* Role Code	Unique code of the role. It cannot be changed once configured

d. To modify the application role, choose **Application Permissions** > **Application Roles**, and select the role.

- Adding members: On the **Members** tab page, click **Add**, select the members to whom you want to assign the role, and click **Save**.

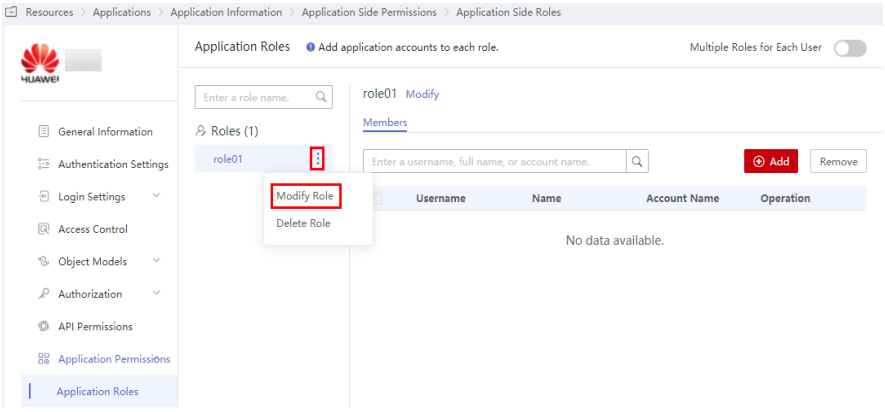
 Copyright © Huawei Technologies Co., Ltd.

Figure 2-59 Adding members



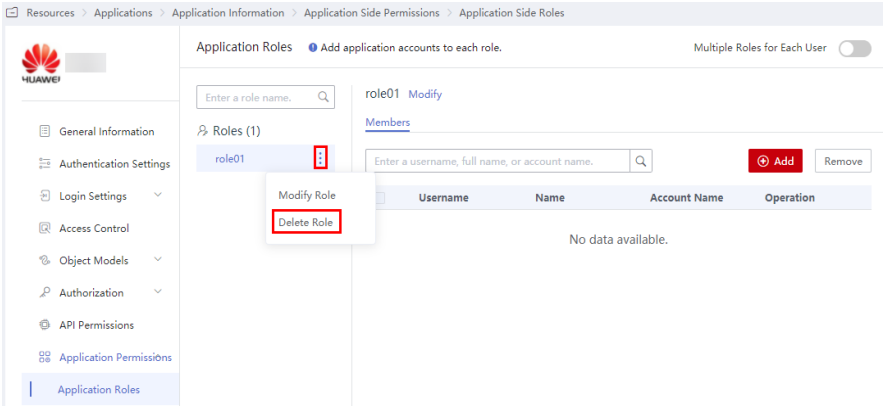
- Adding roles: In the **Roles** pane, click **+**, enter the role name and code, and click **Save**.
- Modifying roles: Click next to the target role, click **Modify Role**, and modify the name.

Figure 2-60 Modifying a role



- Deleting roles: Click next to the target role, click **Delete Role**, and click **OK**.

Figure 2-61 Deleting a role



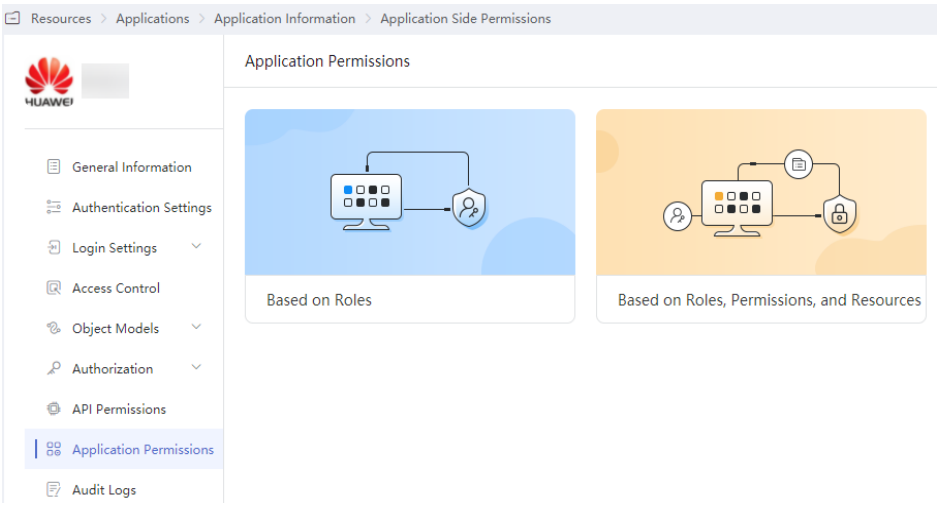
 Copyright © Huawei Technologies Co., Ltd.

- Permissions management by roles, permissions, and resources: 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.

  a. On the application details page, choose **Application Permissions**.

  b. On the **Application Permissions** page, click **Based on Roles, Permissions, and Resources**.

  Figure 2-62 Application permissions management by roles, permissions, and resources

  c. Set the resource information and click **Next**.

  Table 2-13 Resource information

Parameter	Description
Resource Name	(Required) Name of the resource.
Resource Code	(Required) Unique code of the resource.
Data Structure	(Required) Display mode of the resource. The options include **Tree** and **List**.

  d. Define permissions and click **Next**.

  Table 2-14 Permission information

Parameter	Description
Permission Name	(Required) Name of the permission.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Permission Code	(Required) Unique code of the permission.
Resource	(Required) Select the resource created in 3.
Permission Type	(Required) Type of the permission for the selected resource. The options include **Function permission** and **Data permission**.

e. Enter the role name and code, and click **Finish**.

After the configuration is complete, an application role, permission, and resource are created. You can add more application roles, permissions, and resources, modify, or delete them if necessary.

- Application roles: On the **Application Roles** page, add, view, modify, and delete roles, and add members.
- Permissions: On the **Permissions** page, add, view, modify, and delete permissions.
- Application resources: On the **Application Resources** page, add, view, modify, and delete resources.

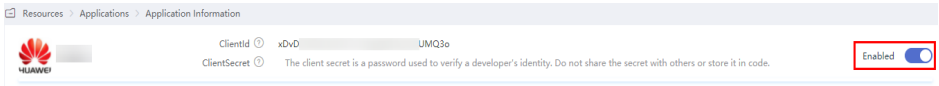
Step 12 View the operation records of the application.

----End

2.3.4 Enabling or Disabling an Application

Disable applications that will not be used. To do this, go to the application information page, click the switch next to **Enabled** in the upper right, and click **OK**.

Figure 2-63 Disabling an application



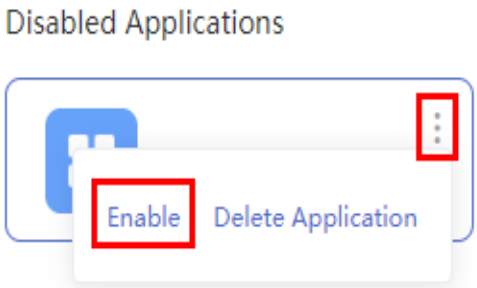
Disabled applications are displayed in the **Disabled Applications** section. To enable an application, locate the application in the **Disabled Applications** area, click in the upper right, click **Enable**, and then click **OK**. The application is no longer displayed in the **Disabled Applications** section.

NOTE

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

Copyright © Huawei Technologies Co., Ltd.

Figure 2-64 Enabling an application



2.3.5 Deleting an Application

CAUTION

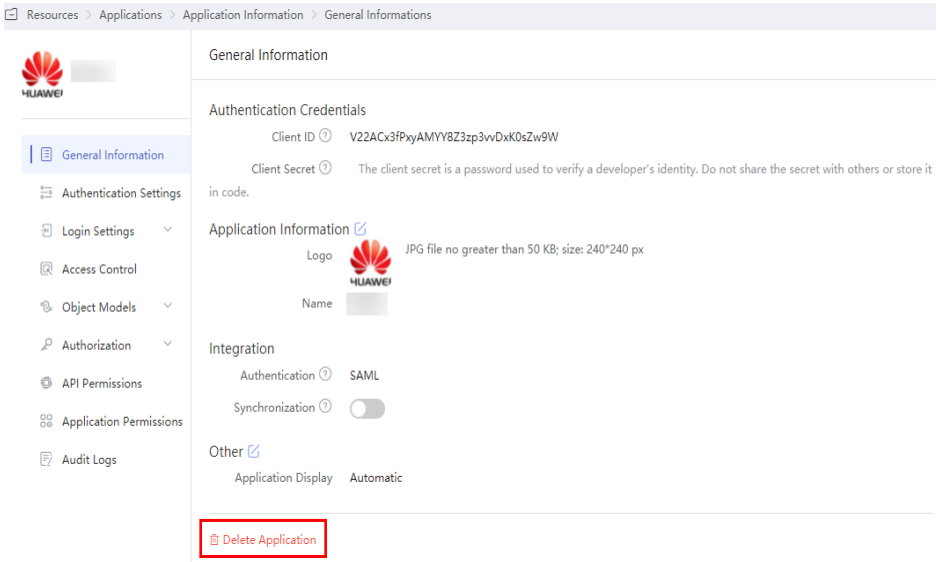
If an application is deleted, all data of the application will be deleted and cannot be recovered.

Step 1 On the **Applications** page, click the application you want to delete.

Step 2 On the application information page, click the application logo or name to go to the application details page.

Step 3 On the **General Information** page, click **Delete Application** at the bottom.

Figure 2-65 Deleting an application



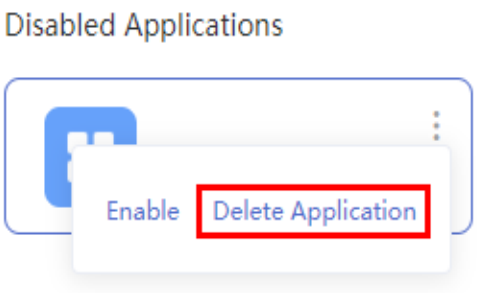
Step 4 Enter the application name and click **OK**.

----End

To delete a disabled application, click ⋮ in the upper right, click **Delete**, and then click **OK**. Deleted applications will no longer be displayed on the **Applications** page.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-66 Deleting an application



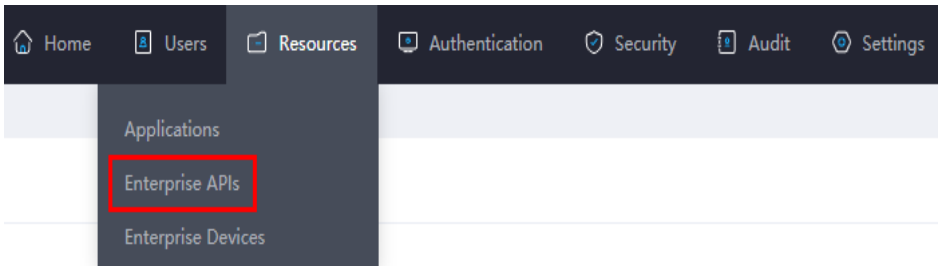
2.3.6 Authorizing Access to Built-in APIs

Authorize API access to specific applications.

Step 1 Log in to the administrator portal.

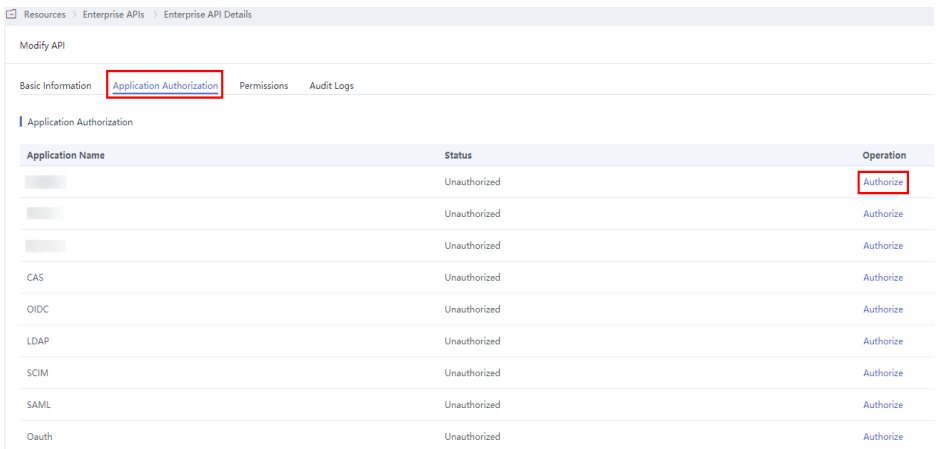
Step 2 In the top navigation pane, choose **Resources** > **Enterprise APIs**.

Figure 2-67 Enterprise APIs



Step 3 On the **Enterprise APIs** page, click **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.

Figure 2-68 Authorizing an application



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 **Application Integration**.

 Copyright © Huawei Technologies Co., Ltd.

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**.

Figure 2-69 Authorizing API access

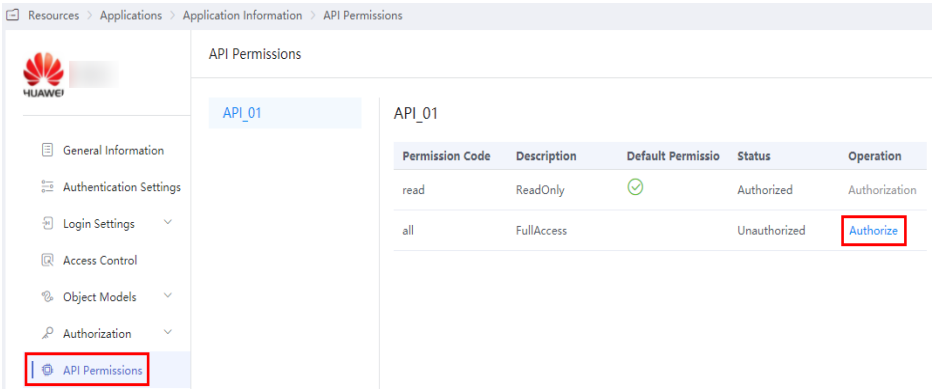


Table 2-15 Mapping between permissions and APIs

Permission Code	Permission 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}	-
		Deactivating a user	PUT /v2/tenant/users/{user_id}/disable	-
		Activating a user	PUT /v2/tenant/users/{user_id}/enable	-
		Changing the password	PUT /api/v2/tenant/users/{user_id}/change-password	-
		Authorizing a user to access a specific application	POST /api/v2/tenant/users/{user_id}/applications/{application_id}/accounts	user_read and read permissions

Copyright © Huawei Technologies Co., Ltd.

Permission Code	Permission Description	API Description	API URL	Remarks
		Querying user details by user ID	GET /api/v2/tenant/users/{user_id}	user_read and read permissions
		Obtaining all application accounts of a user	GET /api/v2/tenant/users/{user_id}/accounts	user_read and read permissions
		Querying users	GET /api/v2/tenant/users	user_read and read permissions
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 by organization ID	GET /v2/tenant/organizations/{org_id}	org_read and read permissions
		Querying organizations	GET /api/v2/tenant/organizations	org_read and read permissions
account_all	Read and write permissions for appli	Adding 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}	-

 Copyright © Huawei Technologies Co., Ltd.

Permission Code	Permission Description	API Description	API URL	Remarks
	cation account management APIs	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 and read permissions
		Querying details of an application account	GET /api/v2/tenant/applications/{application_id}/accounts/{account_id}	account_read and read permissions
		Deactivating an application account	PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}/disable	-
		Activating an application account	PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}/enable	-
app_org_all	Read and write permissions for application organization management APIs	Querying authorized organizations of an application	GET /api/v2/tenant/applications/{application_id}/organizations	app_org_read and read permissions
		Querying details of a virtual organization	GET /api/v2/tenant/applications/{application_id}/organizations/{org_id}	app_org_read and read permissions
		Adding a virtual organization	POST /api/v2/tenant/applications/{application_id}/organizations	-

Copyright © Huawei Technologies Co., Ltd.

Permission Code	Permission Description	API Description	API URL	Remarks
		Modifying a virtual organization	PUT /api/v2/tenant/applications/{application_id}/organizations/{org_id}	-
		Deleting a virtual organization	DELETE /api/v2/tenant/applications/{application_id}/organizations/{org_id}	-
all	Read and write permissions for all OAP APIs	All preceding APIs	-	-

----End

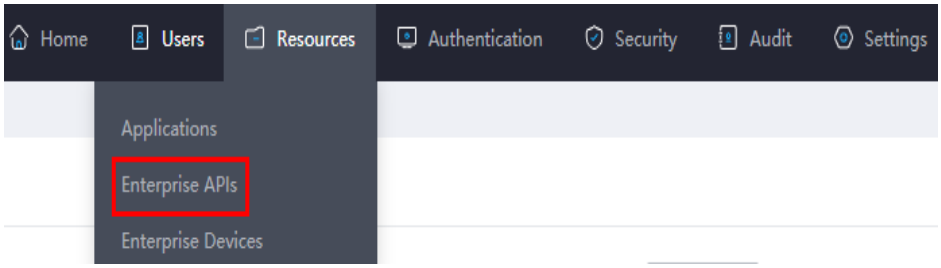
2.3.7 Calling Built-in APIs

Call APIs using authorized applications.

Step 1 Log in to the administrator portal.

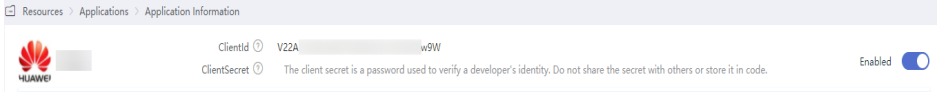
Step 2 In the top navigation pane, choose **Resources** > **Enterprise APIs**.

Figure 2-70 Enterprise APIs



Step 3 Click the target application and obtain its client ID and client secret.

Figure 2-71 Obtaining parameters



Copyright © Huawei Technologies Co., Ltd.

Step 4 Obtain the access token.

Step 5 Call the built-in APIs of OneAccess using the access token.

----End

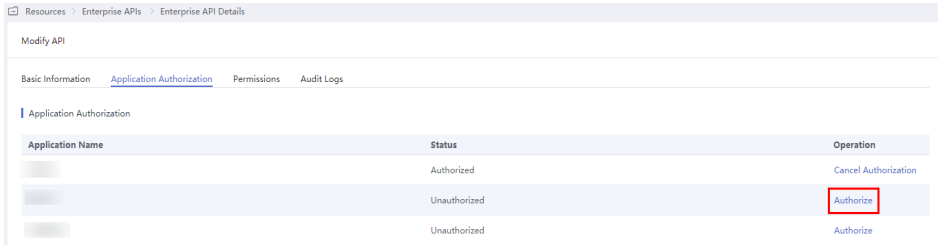
2.3.8 Modifying Built-in APIs

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

Step 1 On the **Enterprise APIs** page, click **Built-in APIs** to go to the enterprise API details page.

Step 2 Authorize applications to call the built-in APIs or cancel authorization. For details about how to add an application, see **Application Integration**.

Figure 2-72 Authorizing an application



Step 3 Modify the API access permissions. Click **Modify** in the **Operation** column of the row that contains the target permission, modify the permission code and description, and determine whether to set the permission as the default.

Figure 2-73 Modifying a permission

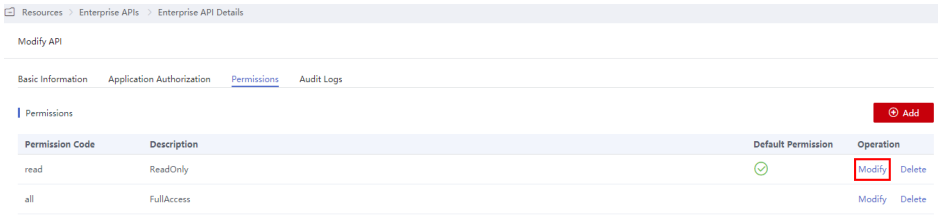


Table 2-16 Permission parameters

Parameter	Description
* Permission Code	Only letters and underscores (_) are allowed.
Description	Description of the permission.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Default Permission	Deselected by default. • 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 4 View the operation records of the APIs.

----End

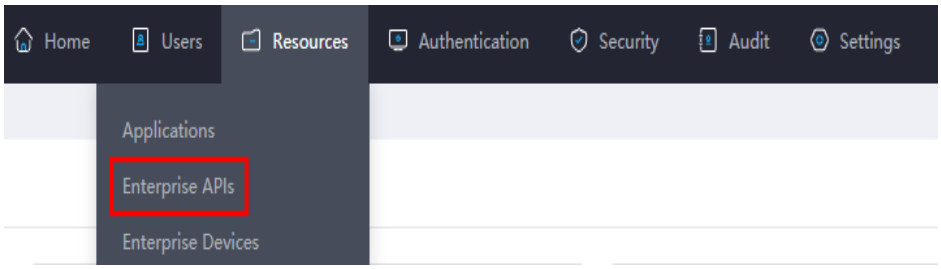
2.3.9 Adding a Custom API

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

Step 1 Log in to the administrator portal.

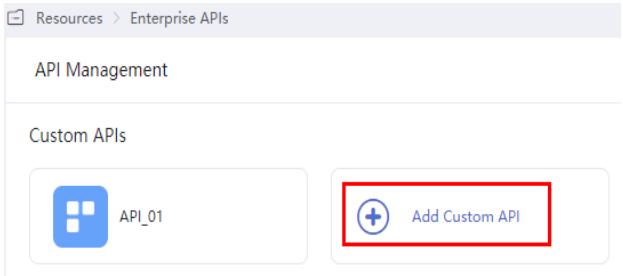
Step 2 In the top navigation pane, choose **Resources** > **Enterprise APIs**.

Figure 2-74 Enterprise APIs



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

Figure 2-75 Adding a custom API



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

----End

2.3.10 Configuring a Custom API

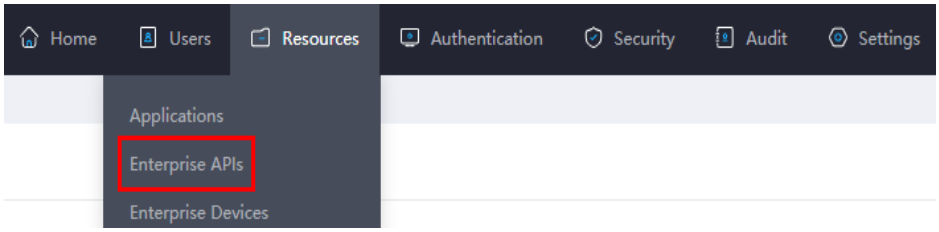
APIs can be called only by applications that have been granted access to them.

Copyright © Huawei Technologies Co., Ltd.

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Resources** > **Enterprise APIs**.

Figure 2-76 Enterprise APIs



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

Step 4 Modify the basic information, including the product logo, name, and description.

Step 5 Grant access of the API to specific applications or cancel their access. 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 Add, modify, or delete permissions for the API.

Step 7 View the operation records of the API.

----End

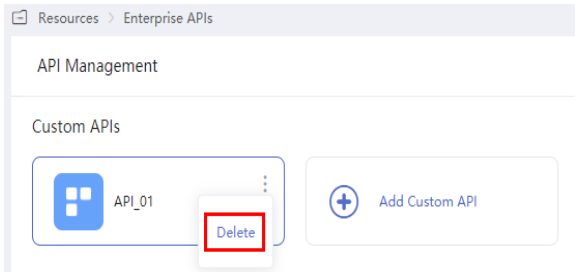
2.3.11 Deleting a Custom API

To delete a custom API, click **Delete** next to the API, and 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.

Figure 2-77 Deleting an API



2.3.12 Adding an Enterprise Device

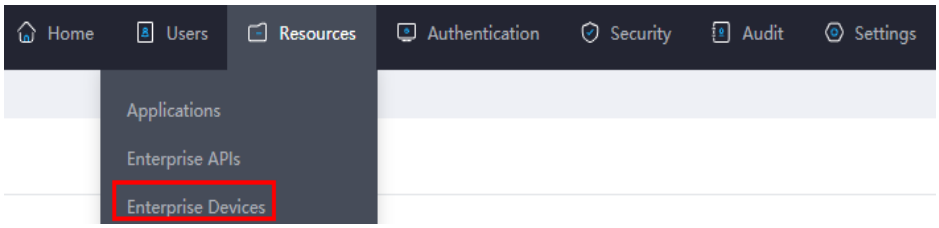
Add enterprise devices in the administrator portal and configure attribute mappings so that users can access applications through the devices.

Step 1 Log in to the administrator portal.

Copyright © Huawei Technologies Co., Ltd.

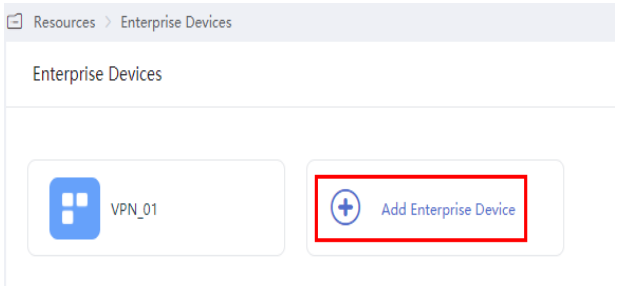
Step 2 In the top navigation pane, choose **Resources** > **Enterprise Devices**.

Figure 2-78 Enterprise Devices



Step 3 On the **Enterprise Devices** page, click **Add Enterprise Device**.

Figure 2-79 Adding an enterprise device



Step 4 Enter the device information.

Table 2-17 Basic information

Parameter	Description
Device Logo	Logo of the enterprise device. Upload an image that does not exceed 50 KB.
Name	Name of the enterprise device.
Type	Device type. The options include **VPN**, **NAS**, and **OTHERS**.
Manufacturer	Device provider. The options include Huawei, Sangfor, H3C, Topsec, Fortinet, and Cisco.
IP Address	Egress IP address for providing VPN services.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Login Authentication	Login authentication mode of the enterprise device. The options include **Local Database**, **AD**, and **OTP**. • **Local Database**: Users are authenticated using their OneAccess username and password during login. • **AD**: Stands for Active Directory. If you select this option, users are authenticated using their AD username and password during login. • **OTP**: Stands for one-time password. It is a password that is valid for only one login session or transaction. **NOTE** If you select **AD**, add an AD authentication provider. For details, see **Adding an Authentication Provider**. If you select **OTP**, configure OTP authentication by referring to **OTP**.
MFA Authentication	Multi-factor authentication (MFA) method. The options include **NONE**, **SMS**, and **OTP**. If you select **SMS** or **OTP**, users need to perform MFA authentication during login. • **NONE**: MFA authentication is not required. • **SMS**: Users need to perform SMS verification during login. • **OTP**: Users need to perform OTP verification during login. **NOTE** If you select **SMS**, configure the SMS gateway. For details, see **SMS Gateway**.
Shared Secret	Secret used for mutual authentication between the VPN service and OneAccess.

Step 5 Click **OK**.

Step 6 To configure mappings for the device added in **Step 5**, click the device on the **Enterprise Devices** page.

Step 7 Click the **Mappings** tab, click **Add Mapping**, and set the parameters required.

Table 2-18 Mapping parameters

Parameter			Description
Attribute Name			(Required) Attribute name of the enterprise device.
Mapping Type	User attribute	User Attribute Name	(Required) Mapping type. The options include **User attribute**, **Fixed attribute value**, and **Dynamic script**. The mapped information varies depending on the mapping type. For example, if you select **User attribute**, select an attribute, such as **userName**.
	Fixed attribute value	Fixed Attribute Value	

Copyright © Huawei Technologies Co., Ltd.

Parameter			Description
	Dynamic script	Dynamic Script	
Scenario			Application scenario of the mapping. • **Success**: Map a user to OneAccess according to this rule if the user passes the authentication on the enterprise device. • **Failure**: Map a user to OneAccess according to this rule if the user does not pass the authentication on the enterprise device. • **Challenge code**: Map a user to OneAccess according to this rule if the user is required to perform MFA authentication.

Step 8 Click **Save**.

Step 9 Click **Audit Logs** to view the operation records of the enterprise device.

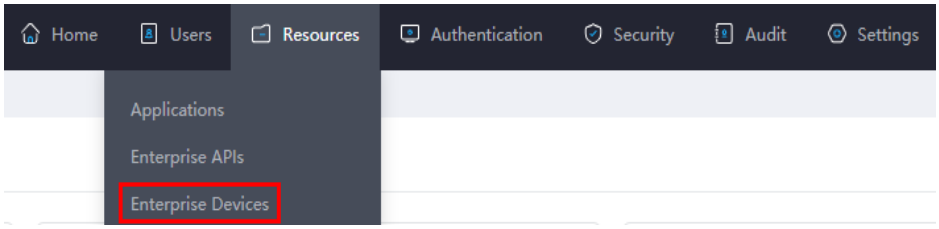
----End

2.3.13 Modifying Device Information

Modify the basic information and attribute mappings of enterprise devices. Log in to the administrator portal.

Step 1 In the top navigation pane, choose **Resources** > **Enterprise Devices**.

Figure 2-80 Enterprise Devices



Step 2 On the **Enterprise Devices** page, click the enterprise device you want to modify.

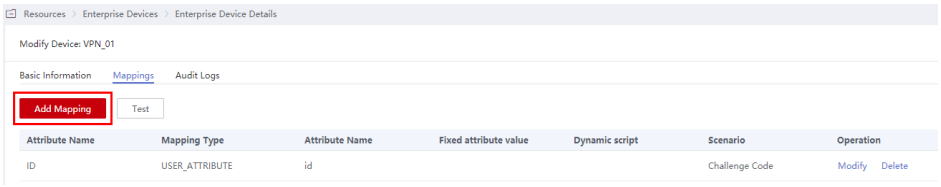
Step 3 Modify the basic information, including the device logo, name, type, and vendor.

Step 4 Add, modify, or delete attribute mappings.

- Adding a mapping: Click **Add Mapping**, set the attribute name, mapping type, and application scenario, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-81 Adding a mapping



- Testing mappings: Click **Test**. On the **Select User** page, enter a username and click **Test**.

Figure 2-82 Testing mappings

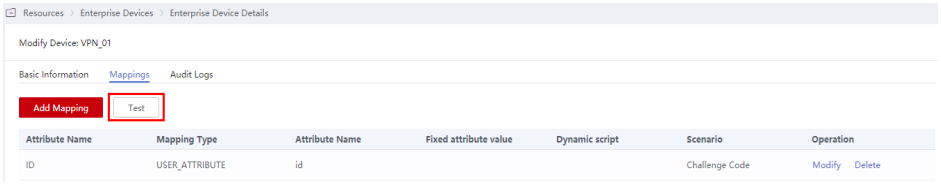
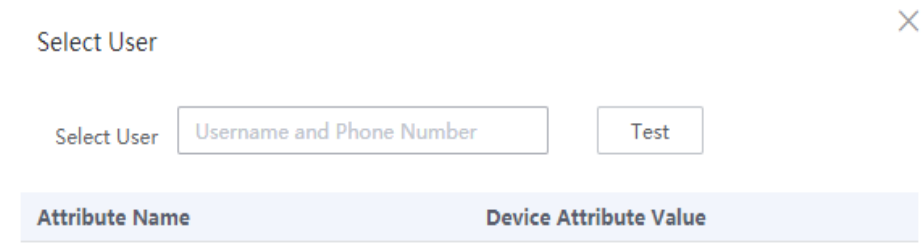
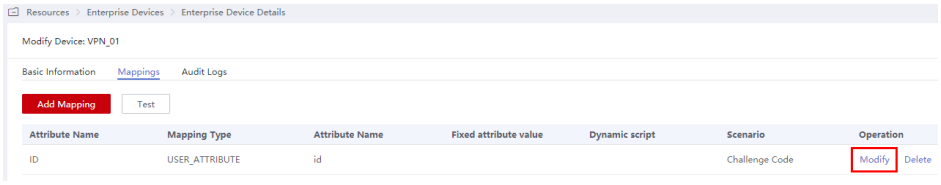


Figure 2-83 Specifying a user



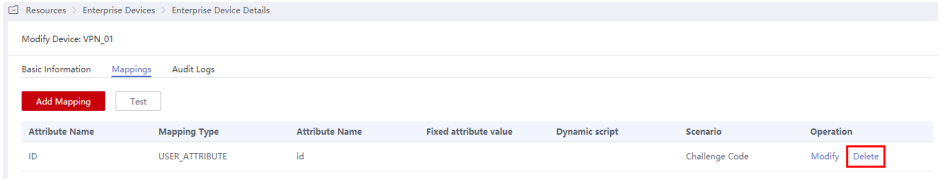
- Modifying a mapping: Click **Modify** in the **Operation** column of the row that contains the target mapping, modify the mapping type and application scenario, and click **OK**.

Figure 2-84 Modifying a mapping



- Deleting a mapping: Click **Delete** in the **Operation** column of the row that contains the target mapping, and click **OK**.

Figure 2-85 Deleting a mapping



----End

 Copyright © Huawei Technologies Co., Ltd.

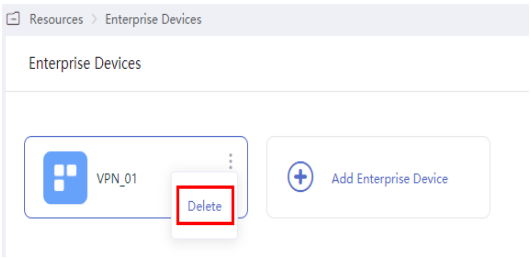
2.3.14 Deleting an Enterprise Device

To delete an enterprise device, click **Delete** next to the device, and click **OK**.

NOTE

Deleted enterprise devices cannot be recovered. Exercise caution when performing this operation.

Figure 2-86 Deleting an enterprise device



2.4 Authentication

2.4.1 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.

CAUTION

You can use both local and third-party authentication providers, and you are advised to select a secure authentication method, such as RADIUS AD, OTP, and SMS. HUAWEI CLOUD will not assume any responsibility for security incidents incurred by insecure authentication methods.

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

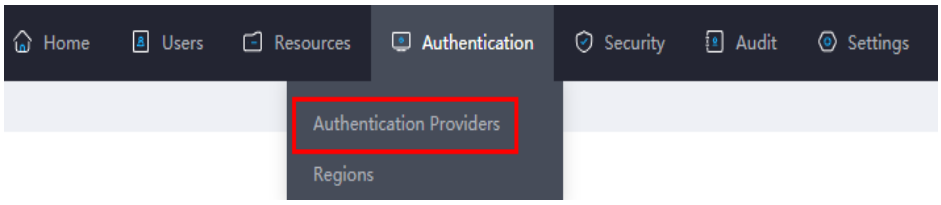
- Ensure that you have administrator permissions for the WeLink open platform.
- Ensure that you have created an application on the WeLink open platform.

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Authentication** > **Authentication Providers**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-87 Authentication Providers



Step 3 On the **Authentication Providers** page, click **WeLink**.

Step 4 Set the WeLink application parameters.

Table 2-19 Configuration parameters

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

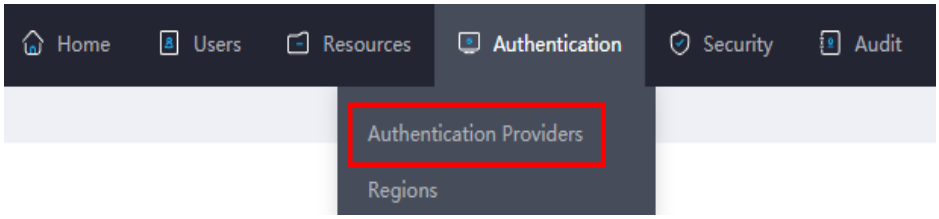
Modifying an Authentication Provider

Modify the settings of an authentication provider.

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Authentication** > **Authentication Providers**.

Figure 2-88 Authentication Providers



Copyright © Huawei Technologies Co., Ltd.

Step 3 On the **Authentication Providers** page, click **WeLink**.

Step 4 Modify the WeLink application parameters.

Step 5 Click **Save**.

----End

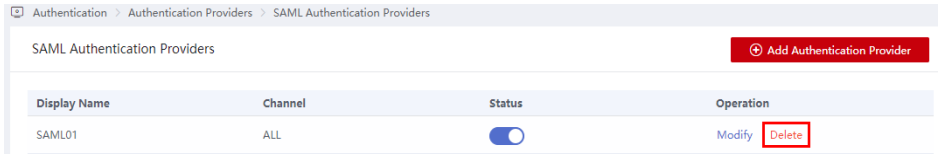
Deleting an Authentication Provider

On the **Authentication Providers** page, click the target authentication provider. On the authentication provider details page, click **Delete** in the **Operation** column and click **OK**.

CAUTION

- 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.

Figure 2-89 Deleting an authentication provider



2.4.2 Regions

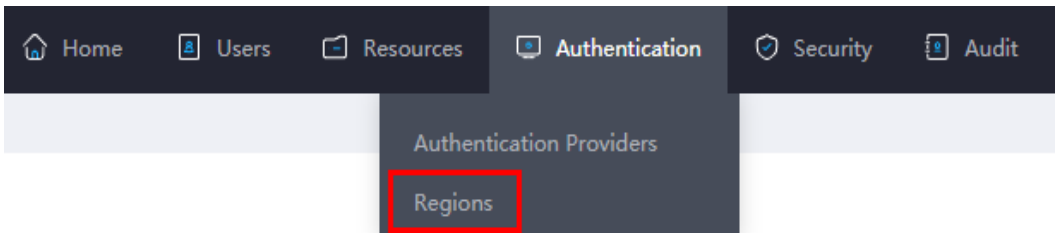
Use regions to allow or deny access of specific users to specific applications.

Adding a Region

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Authentication** > **Regions**.

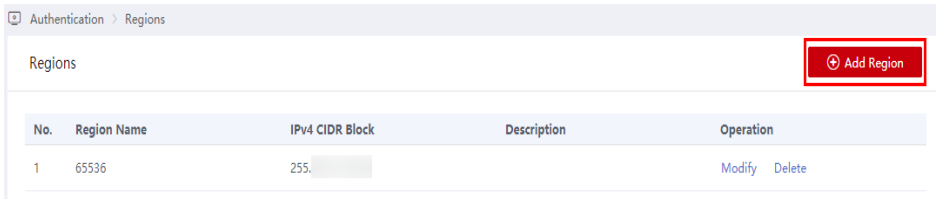
Figure 2-90 Regions



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

Copyright © Huawei Technologies Co., Ltd.

Figure 2-91 Adding a region



Step 4 Enter the region information.

Table 2-20 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.

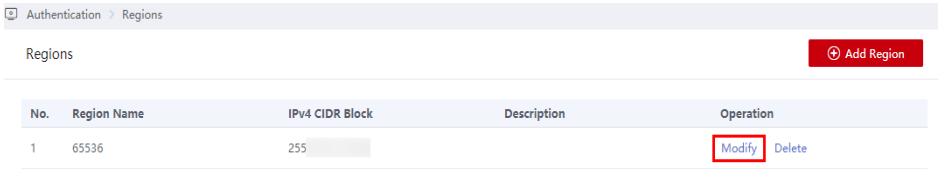
Step 5 Click **Save**.

----End

Modifying a Region

In the region list, click **Modify** in the row that contains the target region, and modify the parameters described in **Table 2-20**.

Figure 2-92 Modifying a region

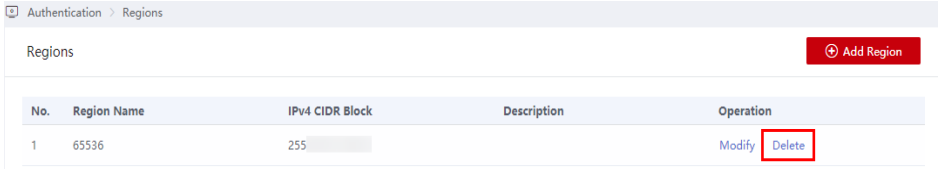


Deleting a Region

In the region list, click **Delete** in the row that contains the target region, and click **OK**.

Deleted regions cannot be recovered. Exercise caution when performing this operation.

Figure 2-93 Deleting a region



Copyright © Huawei Technologies Co., Ltd.

2.5 Security

2.5.1 Administrator Permissions

Add administrators and administrator groups and grant them specific permissions for the administrator portal.

There are super administrators and common 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 in the administrator portal.

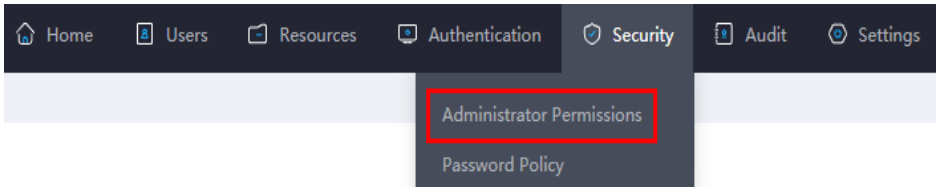
Adding a Super Administrator

Add a super administrator and grant them full permissions for the administrator portal.

Step 1 Log in to the administrator portal.

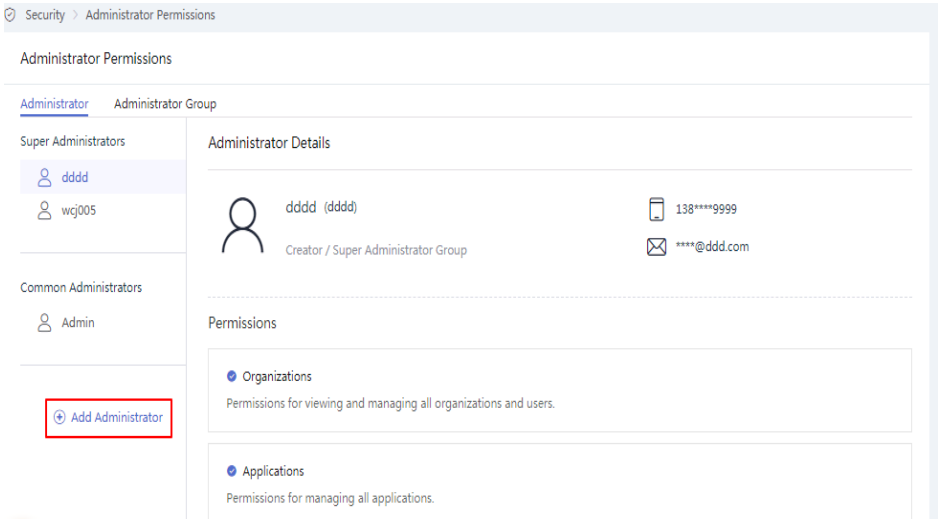
Step 2 In the top navigation pane, choose **Security** > **Administrator Permissions**.

Figure 2-94 Administrator Permissions



Step 3 Click the **Administrators** tab and click **Add Administrator**.

Figure 2-95 Adding an administrator



 Copyright © Huawei Technologies Co., Ltd.

Step 4 Enter the administrator information.

Table 2-21 Administrator information

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

Step 5 Click **Save**.

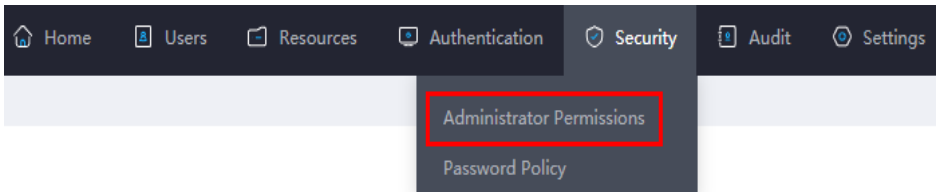
----End

Adding a Common Administrator

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Security** > **Administrator Permissions**.

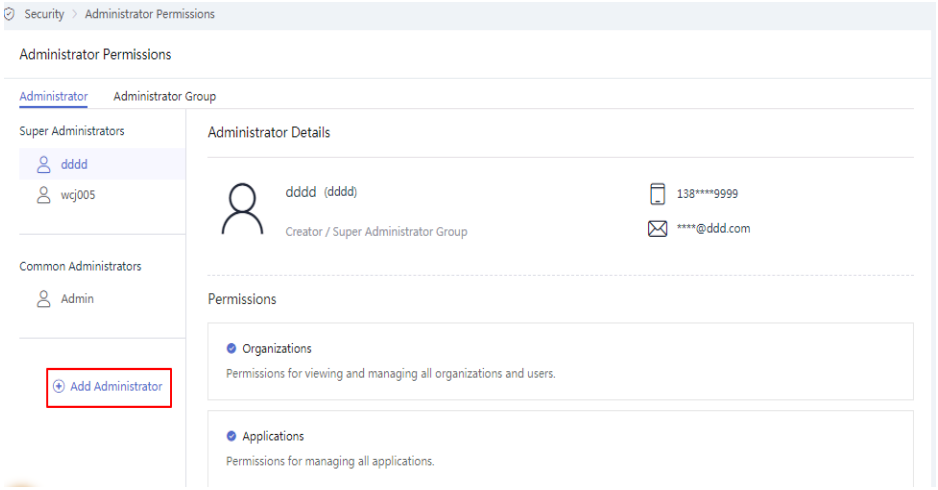
Figure 2-96 Administrator Permissions



Step 3 Click the **Administrators** tab and click **Add Administrator**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-97 Adding an administrator



Step 4 Enter the administrator information.

Table 2-22 Administrator information

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

Step 5 Grant permissions to the administrator.

- **Administrator group**: Select an administrator group. The common administrator then inherits all permissions of the administrator group.
- **Custom**: Grant the common administrator permissions for all or specific organizations, applications, and menus.

Step 6 Click **Save**.

NOTE

You can also select an administrator group and add the common administrator to it. For details about how to add an administrator group, see **Adding an Administrator Group**.

----End

 Copyright © Huawei Technologies Co., Ltd.

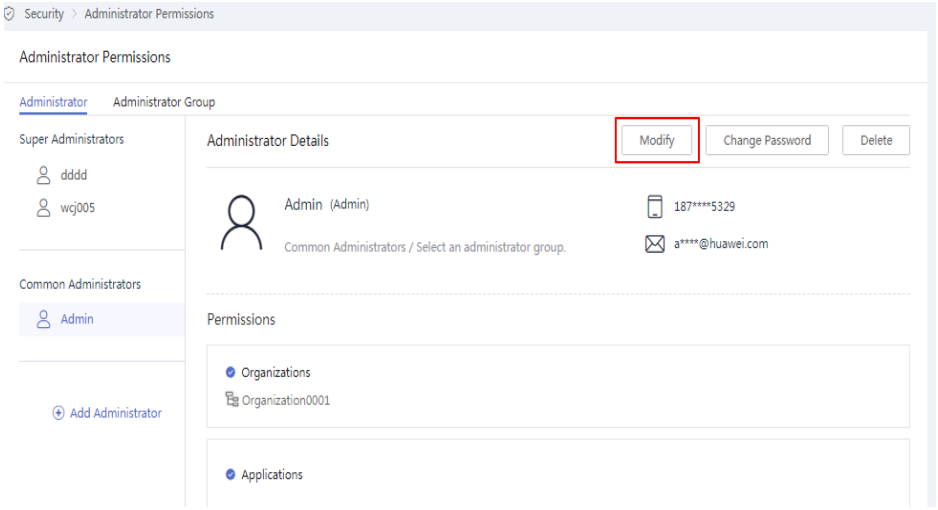
Modifying Administrator Information

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.

Figure 2-98 Modifying an administrator



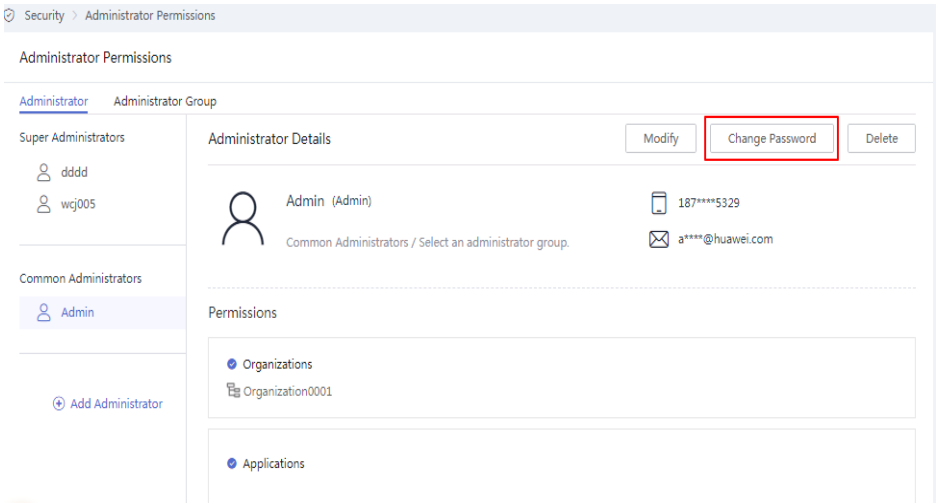
Changing the Password of an Administrator

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

NOTE

To change the password of the enterprise account creator, see **Resetting the Password**.

Figure 2-99 Changing the password



 Copyright © Huawei Technologies Co., Ltd.

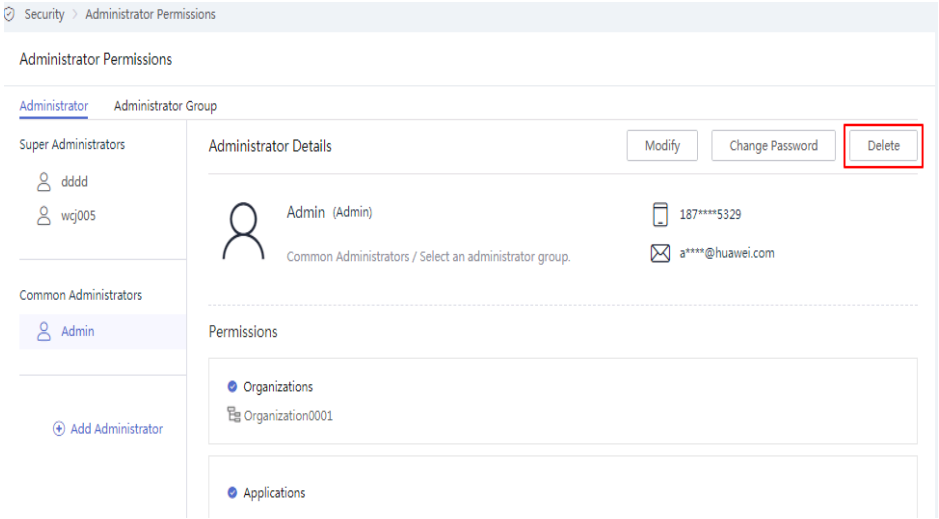
Deleting an Administrator

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

CAUTION

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**.

Figure 2-100 Deleting an administrator



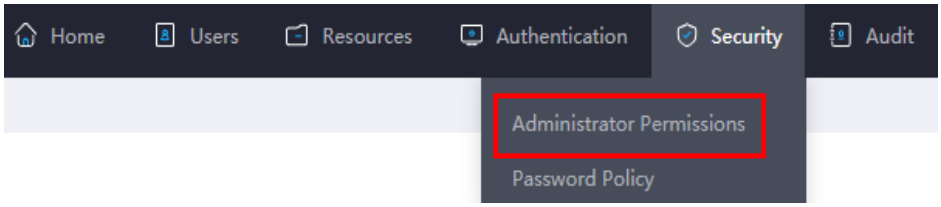
Adding an Administrator Group

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

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Security** > **Administrator Permissions**.

Figure 2-101 Administrator Permissions

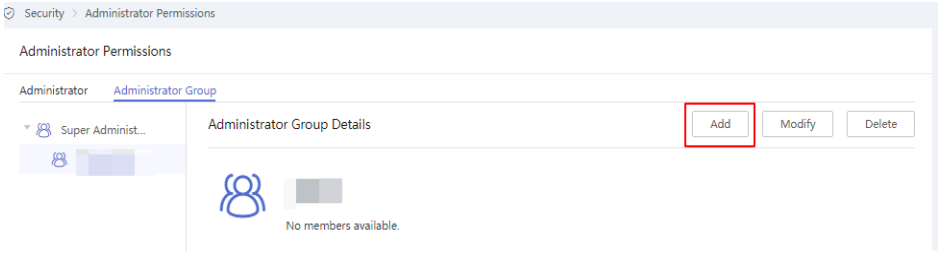


Step 3 On the **Administrator Permissions** page, click the **Administrator Groups** tab.

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

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-102 Adding an administrator group



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

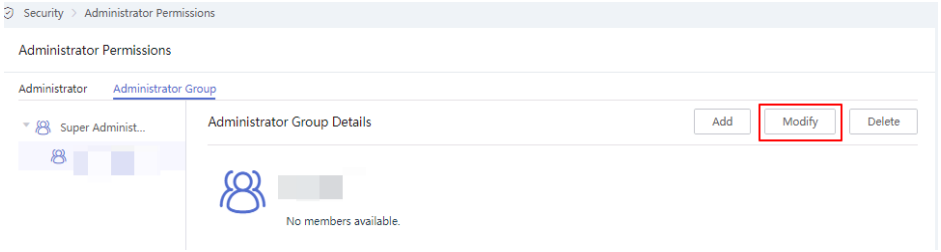
Modifying Administrator Group Information

On the **Administrator Groups** tab page, click the target administrator group, click **Modify**, and modify the administrator group name and permissions.

NOTE

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

Figure 2-103 Modifying an administrator group

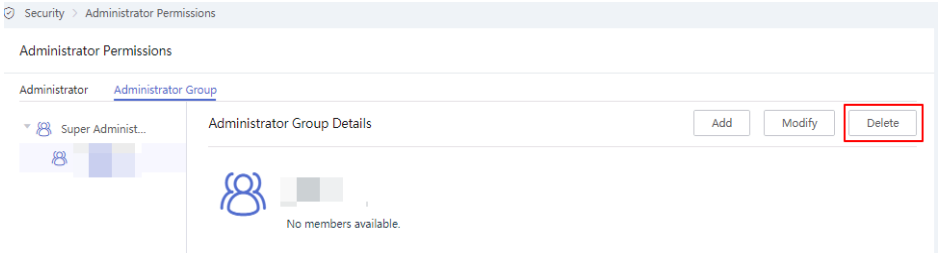


Deleting an Administrator Group

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

On the **Administrator Groups** tab page, click the target administrator group, click **Delete**, and then click **OK**.

Figure 2-104 Deleting an administrator group



 Copyright © Huawei Technologies Co., Ltd.

2.5.2 Password Policy

The password policy consists of **Password Strength**, **Login Security**, and **Advanced 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

- 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.

- 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 for weak passwords. If you enable this option, passwords included in the weak password list are not allowed.

Login Security

- 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.

- 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.

Advanced Settings

- 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.

Copyright © Huawei Technologies Co., Ltd.

- 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.

2.6 Auditing

2.6.1 OneAccess Auditing

OneAccess provides user and administrator operation logs, which can be used to perform security analysis, track resource changes, perform compliance audits, and locate faults.

This section describes how to view, search, and export user and administrator operation logs.

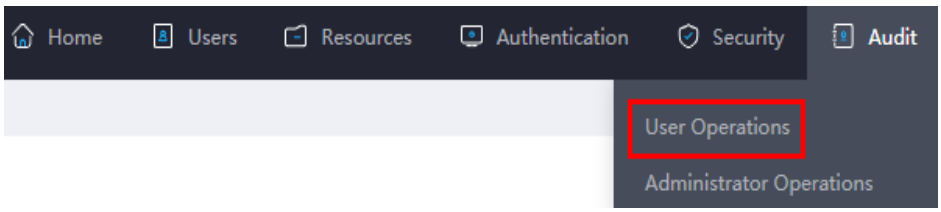
Viewing User Operation Logs

View user operation logs.

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Audit** > **User Operations**.

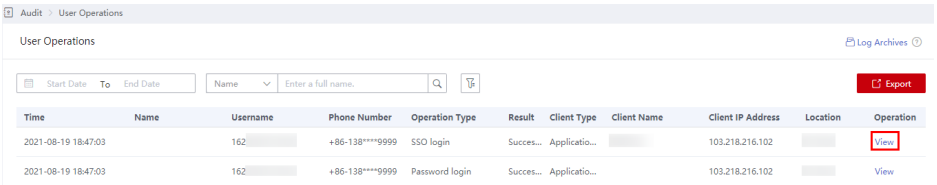
Figure 2-105 User operation logs



Step 3 On the **User Operations** page, click **View** in the **Operation** column of the row that contains a log to view its details.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-106 Viewing log details



----End

NOTE

- You can search user operation logs by time, username, mobile number, operation type, client type, or location.
- To export all user operation logs, click **Export** in the upper right of the log list.
- 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 result, and operation type in each log.

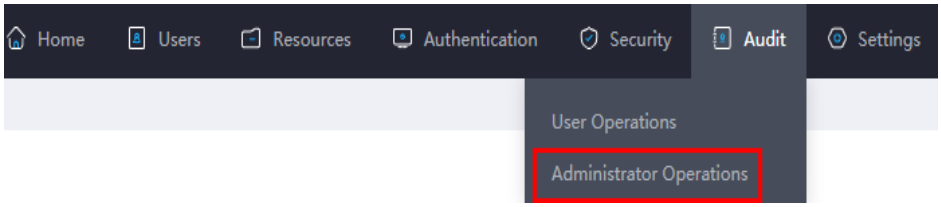
Viewing Administrator Operation Logs

To view administrator operation logs, do as follows:

Step 1 Log in to the administrator portal.

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

Figure 2-107 Administrator operation logs



----End

NOTE

- You can search administrator operation logs by time, username, full name, location, or operation object.
- To export all administrator operation logs, click **Export** in the upper right of the log list.
- 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, content, and location in each log.

2.6.2 HUAWEI CLOUD Auditing

Cloud Trace Service (CTS) records operations performed on cloud resources in your account. The operation logs can be used to perform security analysis, track resource changes, perform compliance audits, and locate faults.

 Copyright © Huawei Technologies Co., Ltd.

It is recommended that you enable the CTS service to record key OneAccess operations, such as buying instances and modifying certificates.

Enabling CTS

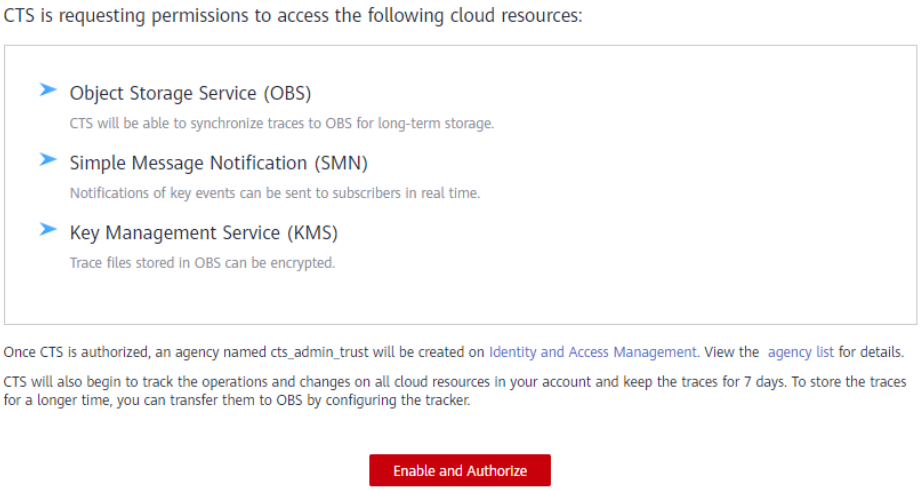
Step 1 Log in to the management console.

Step 2 If you log in to HUAWEI CLOUD using an account, go to **3**. If you log in as an IAM user, request the administrator to grant you the following permissions:

- Security Administrator
- CTS FullAccess

For details, see **Assigning Permissions to an IAM User**.

Step 3 Choose **Service List** > **Management & Governance** > **Cloud Trace Service**.



Step 4 On the displayed authorization page, click **Enable and Authorize**.

NOTE

- When using CTS, you must have the required permissions for relevant operations, but do not need to be granted the **Security Administrator** role again.
- After you enable CTS, the system automatically creates two trackers to record management traces, that is, operations (such as creation, login, and deletion) performed on all cloud resources.
  - In the **current region**, a tracker is created to record management traces of all project-level services deployed in this region.
  - In the **CN North-Beijing4** region, a tracker is created to record management traces of all global services, such as IAM.

----End

View the records of OneAccess operations, such as buying instances and modifying certificates. **Table 2-23** shows the OneAccess operations that can be recorded by CTS.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-23 OneAccess operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Buying an instance	instance	orderInstance
Modifying a certificate	certificate	updateCertificate
Customizing a domain name	domainName	createDomainName
Deleting a custom domain name	domainName	deleteDomainName

Viewing OneAccess Audit Logs

After CTS is enabled, it records key operations performed on OneAccess and other supported services. CTS retains operation records for the last seven days.

Step 1 Perform any operation on the OneAccess console.

Step 2 Log in to the CTS console and view the operation records of OneAccess.

NOTE

OneAccess is a global service, and the operations on OneAccess will be recorded by CTS under the **CN North-Beijing4** region by default. On the CTS console, switch to the **CN North-Beijing4** region and then view OneAccess operation records.

Step 3 Click next to a trace to view its basic information.

Step 4 Click **View Trace** on the right of a trace to view the trace structure. For more information, see **CTS User Guide**.

----End

2.7 Settings

2.7.1 Enterprise Information

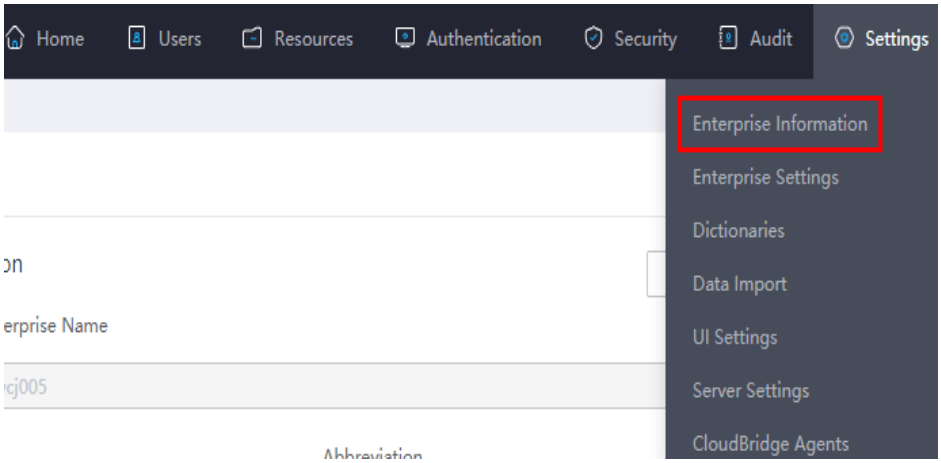
Complete your enterprise information, including industry, staff size, contact, photo number, and address, so that we can provide you services that meet your requirements.

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Settings** > **Enterprise Information**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-108 Enterprise Information



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

----End

2.7.2 Enterprise Settings

OneAccess provides multiple authentication methods to meet your security requirements. You can enable the username rule to ensure a consistent username format. For account security, enable MFA and WeLink-based authentication for the administrator portal. For details, see **General Settings**. To prevent identity theft during login, registration, password resetting, and MFA authentication for VPN access, configure the SMS, voice, email, and DingTalk gateways to verify user identities. For details, see **SMS Gateway**, **Voice Gateway**, **Email Gateway**, and **DingTalk Gateway**.

General Settings

- Username Rule

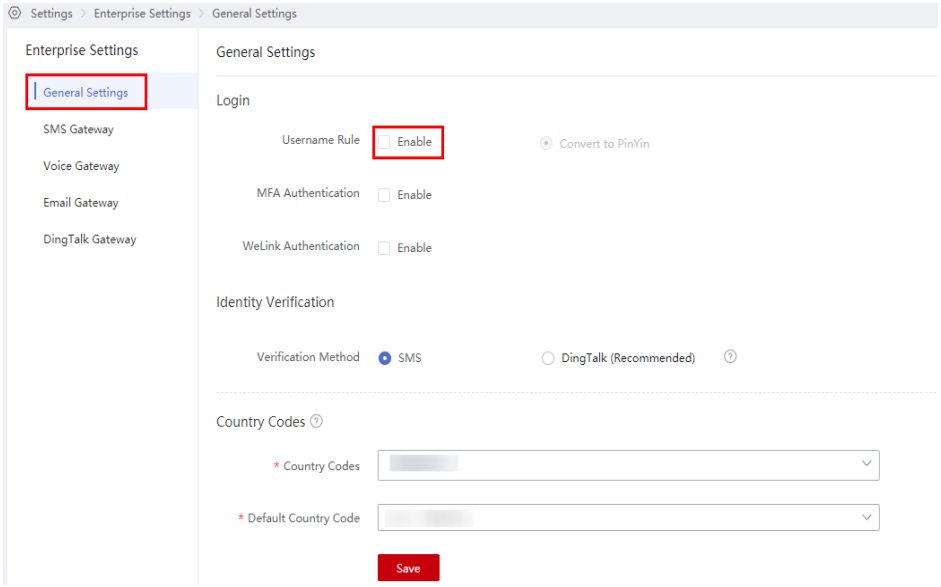
  If you select **Username Rule**, usernames of users you create or import from identity sources will be automatically filled with the corresponding Chinese PinYin. For example, if you enter a Chinese name, the username will be automatically displayed as PinYin. For details about how to add a user, see **Creating a User**.

  NOTE

  After you select **Username Rule**, usernames of new users you created will be renamed using Pinyin.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-109 Enabling the username rule



- 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 2-24 Parameter description

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, ensure that you have created an application on the WeLink open platform.

- Verification Method
  - **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, password resetting (by administrators or users), RADIUS

 Copyright © Huawei Technologies Co., Ltd.

authentication, and MFA authentication. Ensure that you have configured the DingTalk gateway.

SMS Gateway

The SMS gateway helps users obtain SMS messages and verification codes. Configure the **built-in gateway** or **custom gateway**.

- (Optional) Built-in gateway
  - The built-in gateway helps users obtain SMS messages and verification codes. If you select **Built-in gateway**, view the total number of SMS messages and the number of used SMS messages on the **SMS Gateway** page.
  - View the preset templates for different scenarios. Users will receive the preset SMS message or verification code in each scenario.
  - 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.
- (Optional) 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, Xiaoshui Intelligence, and ZTHY. HUAWEI CLOUD SMS service is used for illustration.

  a. On the **SMS Gateway** page, select **Custom gateway**.

  b. In the **Basic Settings** area, specify the SMS service provider as **HUAWEI CLOUD** and set other parameters.

  Table 2-25 Basic settings

Parameter	Description
* Access Key ID	Key of an application registered on the SMS service platform.
* Access Key Secret	Secret of the application.
* Signature	Signature name registered on the SMS service platform.
* Verification Channel No.	Channel No. of a verification code signature.
Notification Channel No.	Channel No. of a notification signature.
* App Access Address	Access address of the application registered on the SMS service platform.

Copyright © Huawei Technologies Co., Ltd.

c. In the **Scenario** section, enter the template ID or code for each scenario, and click **Save**.

Voice Gateway

In addition to SMS verification, OneAccess also supports voice verification. If a user cannot receive an SMS verification code, they can choose to send a voice verification code instead.

- (Optional) Built-in gateway
  - Select **Built-in gateway**, and view the total and used voice messages.
  - View the supported scenarios and preset voice message templates. Users will receive the preset voice messages in different scenarios.
  - 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.
- (Optional) Custom gateway

  Register an account at the voice 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 voice service provider. Supported voice service providers include HUAWEI CLOUD and Alibaba Cloud. For details about how to configure the HUAWEI CLOUD voice gateway, see **Voice Gateway Configuration**.

  a. On the **Voice Gateway** page, select **Custom gateway**.

  b. For **Voice Service Provider**, select **HUAWEI CLOUD** or **Alibaba Cloud**. Then set the required parameters. HUAWEI CLOUD voice gateway is used for illustration.

  Table 2-26 Basic settings

Parameter	Description
* Access Key ID	Access key of an application created on the voice service platform.
* Access Key Secret	Access secret of the application.
* App Access Address	Access address of the application.
* Display Number	Obtain it from the voice service platform.

  c. In the **Scenario** section, enter the template ID or code, and click **Save**.

Email Gateway

The email gateway helps users obtain information through emails during password resetting. If you enable the email gateway, OneAccess generates random

 Copyright © Huawei Technologies Co., Ltd.

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. For details about how to configure the email gateway, see **Email Gateway Configuration**.

- Basic settings: Set the email gateway of your enterprise. All parameters are required.

  Table 2-27 Basic settings

Parameter	Description
* SMTP HOST	Address of the host that provides SMTP services.
* SMTP PORT	Port for providing SMTP services.
* Email Address	Email address of your enterprise, that is, the address from which system emails are sent.
* THEN PERSON NAME	Email sender. The default value is the name of the current user.
* EMAIL PASSWORD	Password of the email account. The default value is the password of the current user.
* ENCRYPTION TYPE	The options include **NONE**, **SSL**, and **TLS**.

- Template settings: Configure the email template for the desired scenario. All parameters are required.

  Table 2-28 Template settings

Parameter	Description
* Template Name	The default name is "Reset Password". Change the name based on the application scenario.
* Email Subject	Enter a custom subject.
* Template	Enter template content.

Copyright © Huawei Technologies Co., Ltd.

DingTalk Gateway

If both SMS verification and voice verification cannot meet your requirements, you can use the DingTalk gateway to send verification codes. After you enable the DingTalk gateway, users can choose DingTalk to send verification codes during login, password resetting, MFA authentication, and RADIUS authentication in the user portal.

- Basic settings

  Table 2-29 Basic settings

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

- Scenarios
  - To modify a template, click **Modify** in the **Operation** column of the row that contains the template, and modify the template content.
  - To test a template, click **Test** in the **Operation** column of the row that contains the template, specify a user, and click **Test**.
  - To copy a template, click **Copy** in the **Operation** column of the row that contains the template.

2.7.3 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.

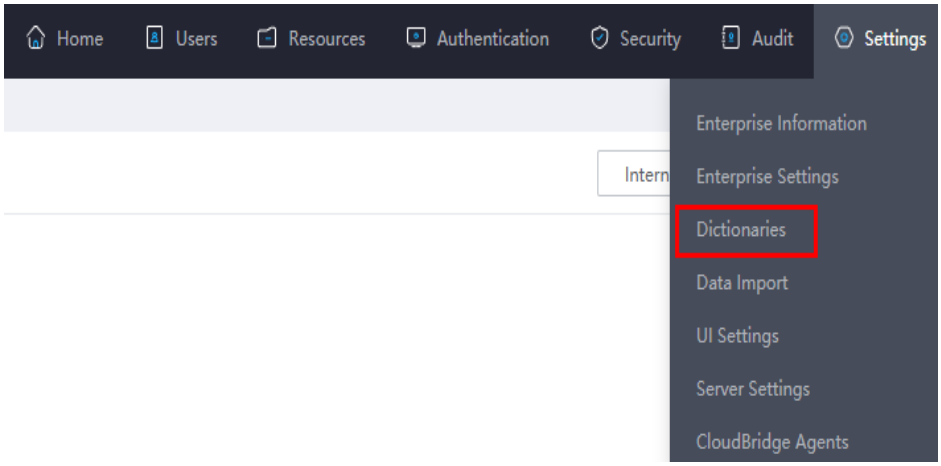
Adding a Dictionary

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Settings** > **Dictionaries**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-110 Dictionaries



Step 3 On the **Dictionaries** page, click **+** at the bottom of the page.

Step 4 Enter the dictionary information and click **Save**.

Table 2-30 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.

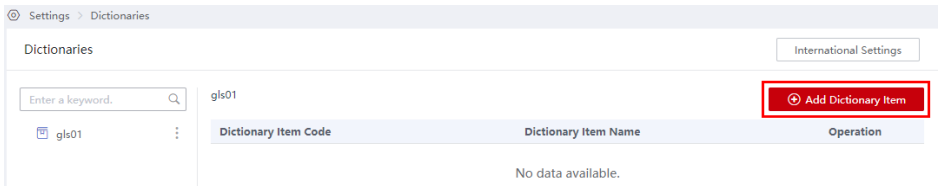
Step 5 Select a dictionary in the left pane.

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 Click **Add Dictionary Item**.

Figure 2-111 Adding a dictionary item



 Copyright © Huawei Technologies Co., Ltd.

Step 7 On the **Add Dictionary Item** page, enter the dictionary item information.

Table 2-31 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 8 Click **Save**.

----End

Modifying a Dictionary

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

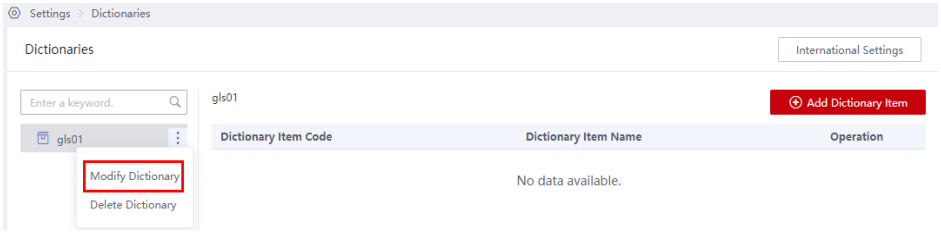
- Modifying a dictionary

  On the **Dictionaries** page, select the dictionary you want to modify, and click **Modify Dictionary**. 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.

  Figure 2-112 Modifying a dictionary

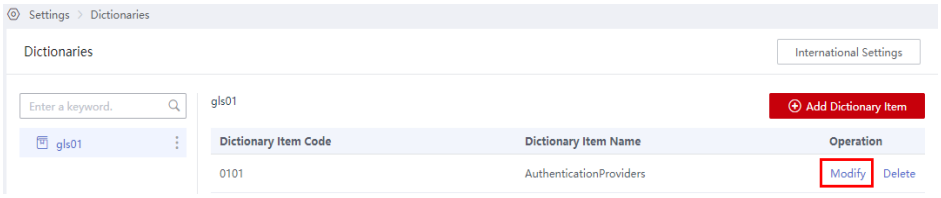
  

- Modifying a dictionary item

  Click **Modify** in the row that contains the target dictionary item, modify the dictionary item name and remarks, and click **Save**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-113 Modifying a dictionary item



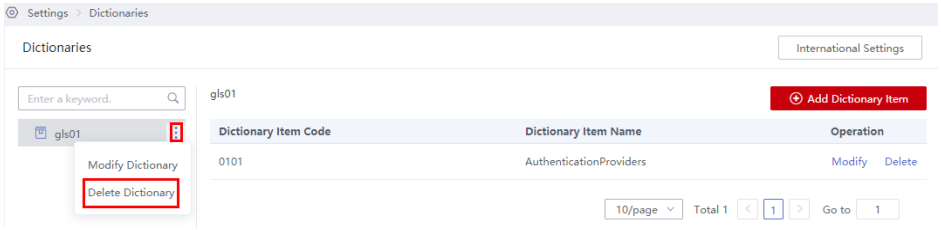
Deleting a Dictionary

On the **Dictionaries** page, select the dictionary you want to delete, click **Delete Dictionary**, and click **OK**.

NOTE

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

Figure 2-114 Deleting a dictionary



2.7.4 Data Import

Import users, organizations, and application accounts in the following scenarios:

- **Importing Users**
- **Importing Organizations**
- **Importing Application Accounts**
- **Importing Shared Accounts**
- **Importing Application Organizations**

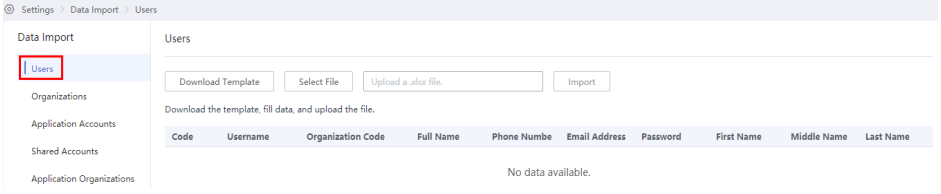
NOTE

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.

Importing Users

1. In the top navigation pane, choose **Settings** > **Data Import**. Then choose **Users** in the left pane.

Figure 2-115 Importing users



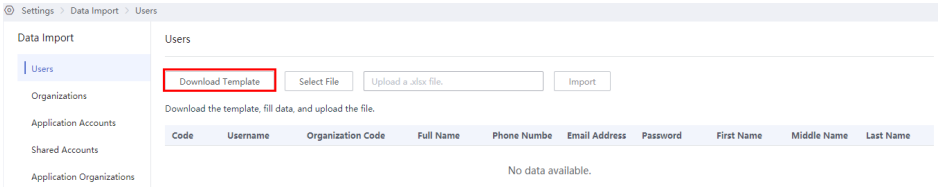
 Copyright © Huawei Technologies Co., Ltd.

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 **Organizations**. To add multiple organizations, see **Importing Application Organizations**.

2. On the **Users** page, click **Download Template**.

Figure 2-116 Downloading the template

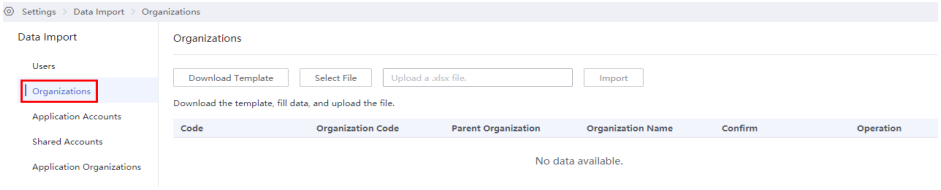


3. Open the downloaded Excel file, add user data to it, and save it.
4. On the **Users** page, click **Select File**, select the file saved in **3**, and click **Open**.
5. Click **Import** to import the user data.

Importing Organizations

1. In the top navigation pane, choose **Settings** > **Data Import**. Then choose **Organizations** in the left pane.

Figure 2-117 Importing organizations

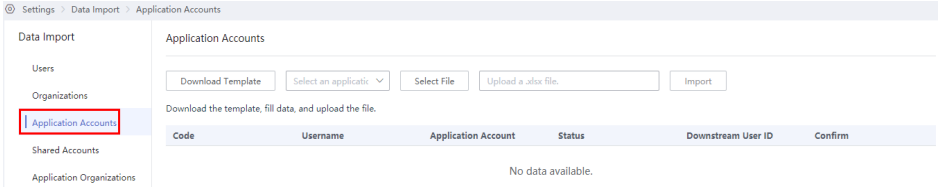


2. On the **Organizations** page, click **Download Template**.
3. Open the downloaded Excel file, add organization data to it, and save it.
4. On the **Organizations** page, click **Select File**, select the file saved in **3**, and click **Open**.
5. Click **Import** to import the organization data.

Importing Application Accounts

1. In the top navigation pane, choose **Settings** > **Data Import**. Then choose **Application Accounts** in the left pane.

Figure 2-118 Importing application accounts



 Copyright © Huawei Technologies Co., Ltd.

NOTE

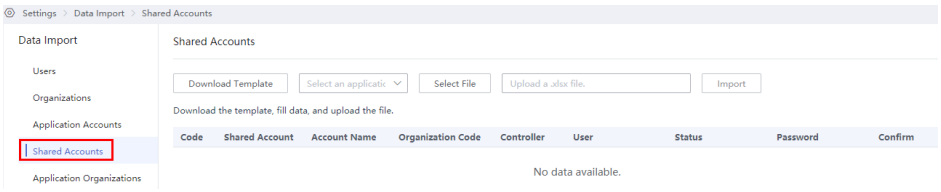
Before importing application accounts, ensure that the application for which you want to import accounts already exists. For details about how to add an application, see **Adding an Application**.

2. On the **Application Accounts** page, click **Download Template**.
3. Open the downloaded Excel file, add account data to it, and save it.
4. On the **Application Accounts** page, click **Select File**, select the file saved in **3**, and click **Open**.
5. Click **Import** to import the application account data.

Importing Shared Accounts

1. In the top navigation pane, choose **Settings** > **Data Import**. Then choose **Shared Accounts** in the left pane.

Figure 2-119 Importing shared accounts



NOTE

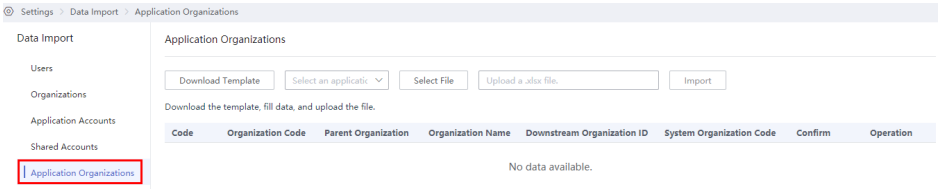
Ensure that the application to which the accounts to import will belong already exists. For details about how to add an application, see **Adding an Application**.

2. On the **Shared Accounts** page, click **Download Template**.
3. Open the downloaded Excel file, add account data to it, and save it.
4. On the **Shared Accounts** page, click **Select File**, select the file saved in **3**, and click **Open**.
5. Click **Import** to import the shared account data.

Importing Application Organizations

1. In the top navigation pane, choose **Settings** > **Data Import**. Then choose **Application Organizations** in the left pane.

Figure 2-120 Importing application organizations



NOTE

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**.

 Copyright © Huawei Technologies Co., Ltd.

2. On the **Application Organizations** page, click **Download Template**.
3. Open the downloaded Excel file, add application organization data to it, and save it.
4. On the **Application Organizations** page, click **Select File**, select the file saved in **3**, and click **Open**.
5. Click **Import** to import the application organization data.

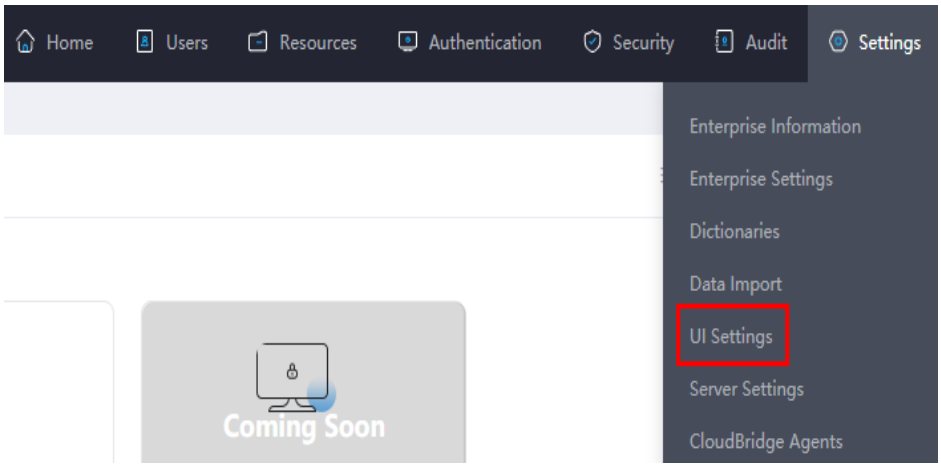
2.7.5 UI Configuration

You can customize the login and registration 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. A custom plan defines the transparency of the header, body, and footer areas and the theme color, color inversion, buttons, and form position.

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Settings** > **UI Settings**.

Figure 2-121 UI Settings



Step 3 On the **UI Settings** page, click **Global Settings**. Then click **Modify** on the **UI Settings** page.

Table 2-32 Global parameter configuration

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 x 180 pixels.
	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 x 140 pixels.

 Copyright © Huawei Technologies Co., Ltd.

Global Parameter		Description
	Website Favicon	Website icon. Upload an ICO file whose size does not exceed 50 KB. The recommended image size is 32 x 32 pixels.
User Portal Login Page	Man-Machine Verification	Verification method used on the login page. Currently, only slide 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.
User Portal Homepage - Top Area	Background Color	Color in which the top area of the user portal homepage will be displayed.
	Title Text	Text to be displayed in the top area of the user portal homepage.
International Settings	Languages	Languages supported by the user portal.
	Default Language	Default language of the user portal.
Verification Code	Length	Length of the verification code used for SMS verification in the user portal. 4-digit and 6-digit verification codes are supported.
	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 Customize the login and registration pages of the user portal for PC.

- User portal login page: On the **UI Settings** page, choose **CustomizeLogin Page** under **User Portal for Web**, click **Add Custom Plan**, and customize the UI settings.
- User portal registration page: On the **UI Settings** page, choose **CustomizeRegistration Page** under **User Portal for Web**, click **Add Custom Plan**, and customize the UI settings.

Table 2-33 describes all parameters for web and mobile devices. Some parameters are available only for either of them.

Table 2-33 Custom UI parameters

Area	Parameter	Description
UI layout	Background Image	Background image of the user portal. The recommended image size is 1920 x 1080. Select a background image provided by the system or upload one.

Copyright © Huawei Technologies Co., Ltd.

Area	Parameter	Description
	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.
	Center Area Font Color	Color of the text (such as **Forgot Password** and **Log In with** on the user portal login page. This parameter is available only for the login and registration page settings of the user portal for PC.
Top Area	Top Banner	Indicates whether to display the top area of the user portal. This parameter is available only for the login and registration page settings of the user portal for PC and the login page settings for mobile devices.
	Background Color	Background color of the top area in the user portal.
	Font Color	Color of the text to be displayed in the top area of the user portal.
	Icon	Indicates whether to display the enterprise icon in the top area of the user portal. This parameter is available only for the login page settings of the user portal for mobile devices.
Bottom Area	Bottom Area	Indicates whether to display the bottom area of the user portal. This parameter is available only for the login and registration page settings of the user portal for PC.
	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.
	Font Color	Color of the text to be displayed in the bottom area of the user portal.

Copyright © Huawei Technologies Co., Ltd.

Area	Parameter	Description
	Bottom Font	Text to be displayed in the bottom area of the user portal. This parameter is available only for the login page settings of the user portal for mobile devices.
	Bottom Link Font Color	Color of the links to be displayed in the bottom area of the user portal. This parameter is available only for the registration page settings of the user portal for mobile devices.
	user Agreement	Agreement to be displayed on the registration page of the user portal. This parameter is available only for the registration page settings of the user portal for mobile devices.
	privacy Policy	Privacy policy that users must agree to register with the user portal. This parameter is available only for the registration page settings of the user portal for mobile devices.
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.
	Background Color	Color of the form area. This parameter is available only for the login and registration page settings of the user portal for PC.
	Input Field Background Color	Color of the text boxes in the form area. This parameter is available only for the login and registration page settings of the user portal for PC.
	Default Font Color	Color of the texts to be displayed in the form area.
	Theme Color	Theme color of the form area.
	user Agreement	Agreement to be displayed on the registration page of the user portal. This parameter is available only for the registration page settings of the user portal for PC.

Copyright © Huawei Technologies Co., Ltd.

Area	Parameter	Description
	privacy Policy	Privacy policy that users must agree to register with the user portal. This parameter is available only for the registration page settings of the user portal for PC.
	Form Hint Font Color	Color of the messages to be displayed in the login form of the user portal. This parameter is available only for the login and registration page settings of the user portal for mobile devices.
	Form Link Font Color	Color of the links to be displayed in the login form of the user portal. This parameter is available only for the login page settings of the user portal for mobile devices.

Step 5 Customize the user portal login and registration pages for mobile devices such as mobile phones and tablets.

- User portal login page

  On the **UI Settings** page, choose **CustomizeLogin Page** under **User Portal for Mobile**, click **+** under **Custom Plans**, and customize the UI settings. For details about the UI parameters, see **Table 2-33**.

- User portal registration page

  On the **UI Settings** page, choose **CustomizeRegistration Page** under **User Portal for Mobile**, click **Add Custom Plan**, and customize the UI settings. For details about the UI parameters, see **Table 2-33**.

----End

2.7.6 Service Configuration

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

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, HUAWEI CLOUD supports software-based virtual MFA devices, which are application programs running on smart devices such as mobile 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.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-34 Parameter configuration

Parameter	Description
Encryption Algorithm	Default algorithm: HMACSHA1. This parameter cannot 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 cannot 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.

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.

IdP

To establish a SAML-based trust relationship with an application, upload the metadata file of the IdP to the SP server. For details about how to upload the metadata, see the documentation of the SP.

Click **IdP** on the **Server Settings** page, and click **Download IdP Metadata** in the upper right. Then upload the downloaded metadata file to your SP server.

Table 2-35 IdP service parameters

Parameter	Description
IDP EntityId	Unique identifier of the IdP.
SSO URL	URL for SSO.
IdP Logout URL	URL for SLO.
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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Request Signature	By default, this option is enabled.
Assertion Signature	By default, this option is enabled.
Assertion Encryption	By default, this option is disabled.

OIDC

To establish an OIDC-based trust relationship with an application, obtain the required port information.

Click **OIDC**. On the **OIDC** page, click **OIDC Discovery** in the upper right corner to view the OIDC data.

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.

CAS

To establish a CAS-based trust relationship with an application, view and configure the CAS service information.

Click **CAS**, and view the CAS configuration parameters.

Parameter	Description
Server Prefix	Prefix of the CAS server URL.
Login URL	Login URL of the CAS server.
ST Validity Period	Validity period of a returned service ticket (ST). Set a validity period from 3 to 15 minutes.

RADIUS

To configure enterprise devices, view the RADIUS configuration information.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
RADIUS Server	URL of the RADIUS Server.
Port	Authentication port of the RADIUS server for interconnecting with enterprise devices.
Supported Protocols	Protocols supported by the RADIUS server when interconnecting with enterprise devices. The protocols include: **PAP**, **CHAP**, **MS-CHAPv1**, and **MS-CHAPv2**.

API Authentication

To register open APIs with OneAccess, view the API authentication settings and configure them for interaction with your applications.

Parameter	Description
Signature Algorithm	Only the default value can be used.
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 **Modify** to set a key.
Validity Period	Validity period of the ID token. The default value is 30 minutes.

2.7.7 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 protecting network entities from interception and repeated attacks.

Currently, CloudBridge agents can be used only with the AD authentication provider. This section describes how to connect an AD authentication provider to OneAccess through a CloudBridge agent.

Prerequisites

Ensure that you have the capabilities required to deploy CloudBridge agents.

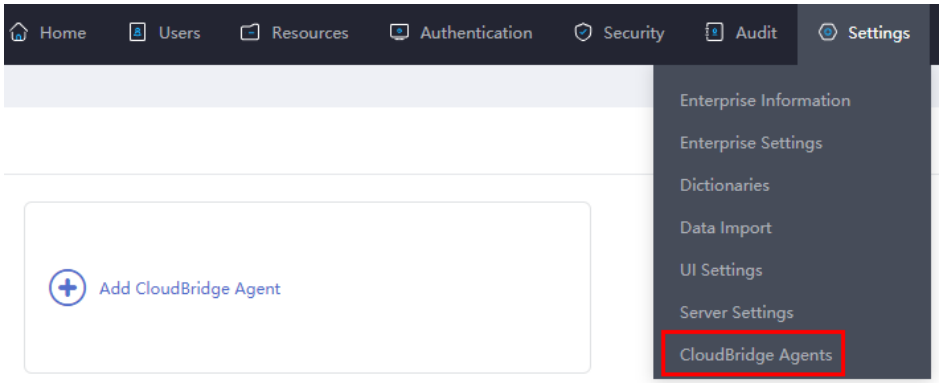
 Copyright © Huawei Technologies Co., Ltd.

Procedure

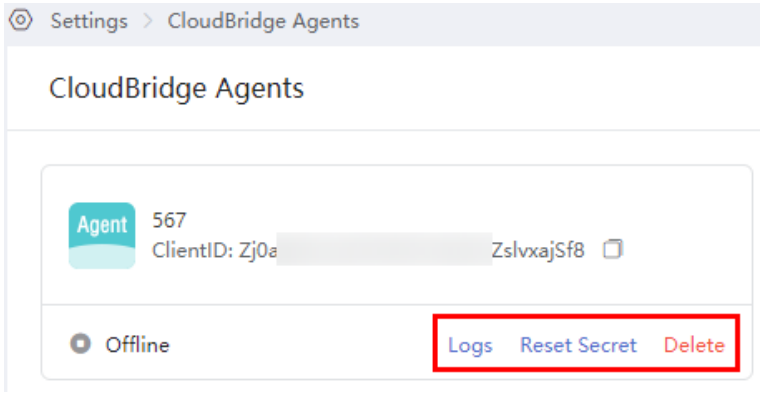
Step 1 Deploy the AD service, and create a domain account to establish an enterprise management system. For details, see **Setting Up an AD Server** and **Creating a Domain Account**.

Step 2 Add a CloudBridge agent.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Settings** > **CloudBridge Agents**.



3. On the **CloudBridge Agents** page, click **Add CloudBridge Agent**. Then set the agent name and type, and click **OK**.



NOTE

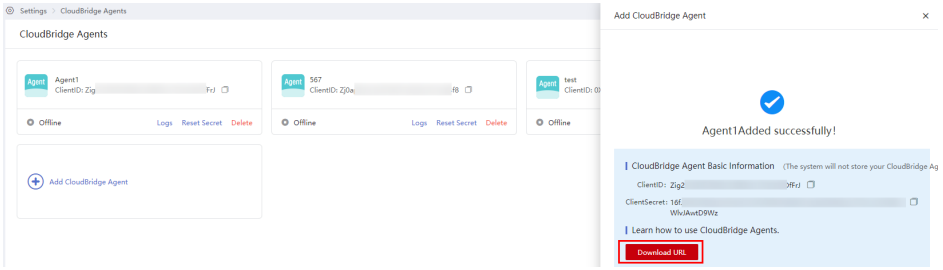
- The system automatically generates a client ID and secret for the CloudBridge agent you created. Keep the client ID and secret properly.
- If you have forgotten the client secret, click **Reset Secret** next to the target agent to generate a new one. The original secret will become invalid after the resetting. Exercise caution when performing this operation.
- To view the connection logs, click **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.

The following procedure uses CentOS Linux release 8.0.1905 as an example to describe how to deploy the CloudBridge agent.

1. Download the **deployment package**.

 Copyright © Huawei Technologies Co., Ltd.



2. Upload the deployment package to the target server.
3. Run **unzip -od** *{Directory for storing decompressed files}* **cloudAgent.zip** to decompress the deployment package. Specify a unique directory to ensure successful deployment. For details about the deployment package, see **Table 2-36**.

Table 2-36 Directory structure

Name	Description
agent.sh	Automatically runs the CloudBridge agent upon startup.
cloudAgent.jar	Deployment package of the CloudBridge agent.
cloudBridge.sh	Used to manually run the CloudBridge agent.
config	Directory for storing the configuration file (**application.yml**) of the CloudBridge agent.
log	Directory for storing the log file (**agent.log**) of the CloudBridge agent.

4. 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**.

 Copyright © Huawei Technologies Co., Ltd.

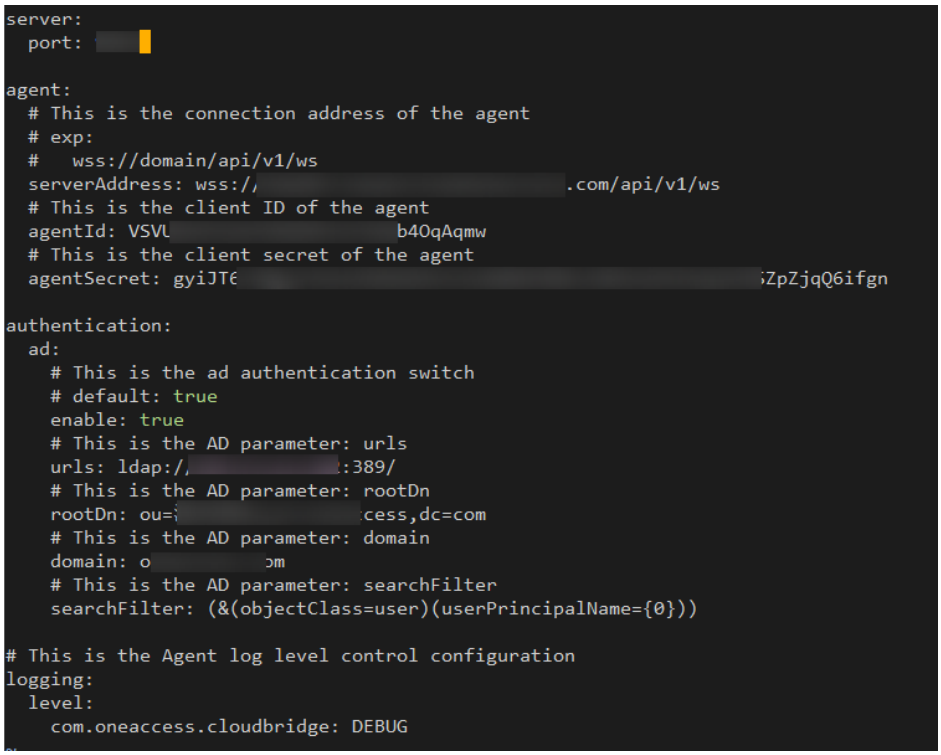


Table 2-37 Configuration parameters

Parameter	Description
* 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 in OneAccess**.
* rootDn	AD node used to authenticate users. To obtain this parameter, see **Adding an AD Authentication Provider in OneAccess**.
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 in OneAccess**.

5. Once configured, run **./cloudBridge.sh start** for the **cloudBridge.sh**. The message "Starting Agent Success." indicates that the agent is started successfully.

 Copyright © Huawei Technologies Co., Ltd.

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 running upon startup, run **./agent.sh install** for the **agent.sh** file. The message "The Agent service installed successfully, need to reboot will take effect." indicates that the installation is successful.
- To uninstall the agent, run **./agent.sh uninstall**. The message "uninstall Agent Success." indicates that the agent is uninstalled successfully.

6. Obtain logs from the **log/agent.log** file.

Step 4 Add an AD authentication provider.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Authentication** > **Authentication Providers**. Then click **AD**.
3. On the **AD Authentication Providers** page, click **Add Authentication Provider** in the upper right and set the required parameters.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-122 Adding an AD authentication provider

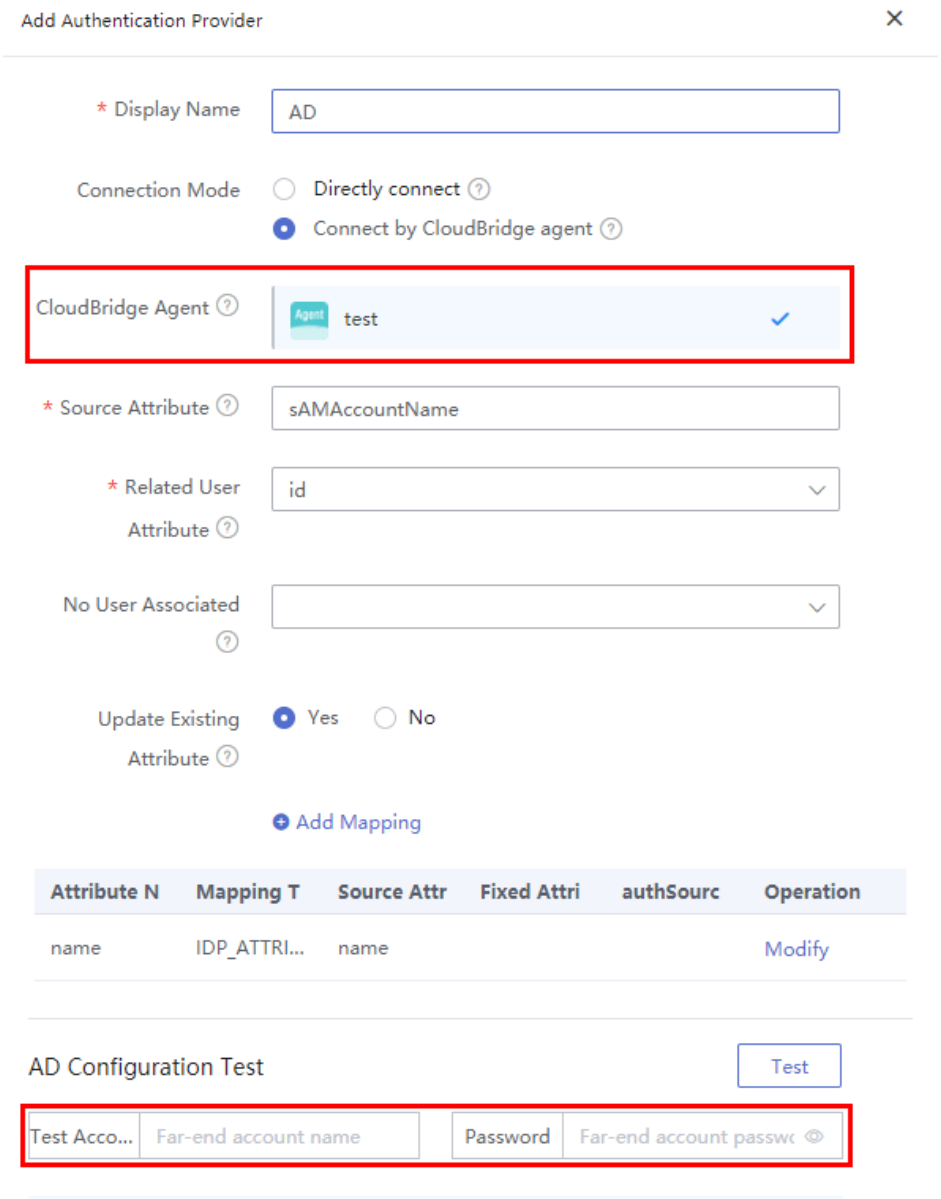


Table 2-38 Configuration parameters

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**.

 Copyright © Huawei Technologies Co., Ltd.

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.

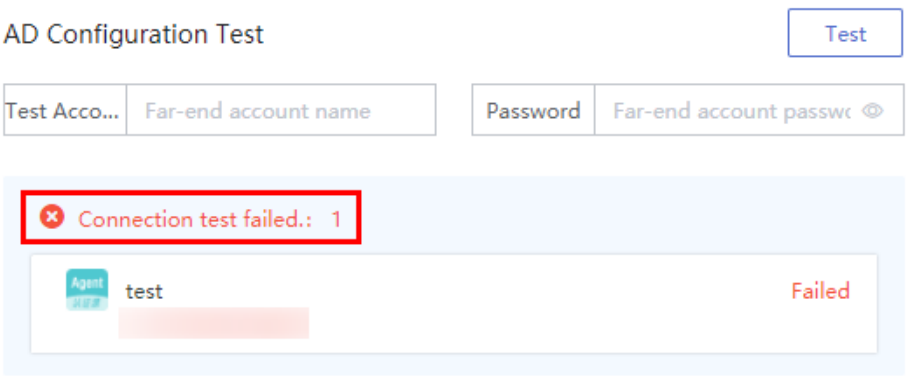
To map other attributes, such as name, set **No User Associated** to **Automatically create users**, and add the desired mappings. For details, see **Table 2-39**.

Table 2-39 Mapping parameters

Parameter	Description
User Attribute	Attribute in OneAccess to which AD will map. For example, **email**.
Mapping Type	Mode of user attribute mapping between OneAccess and AD.
Authentication Provider Attribute Name	Name of an AD user attribute.

4. Enter a test account and password and click **Test** to check the connectivity.

   If you have selected multiple CloudBridge agents (see **Figure 2-122**), the system checks the connectivity of each agent after you click **Test**. If the check fails, view the cause.



 Copyright © Huawei Technologies Co., Ltd.

Step 5 Enable AD authentication for an application. For details, see **Enabling AD Authentication in OneAccess**.

Step 6 Verify login using an AD account. For details, see **Verifying Login Through AD Authentication**.

----End

 Copyright © Huawei Technologies Co., Ltd.

3 Common User Guide

Logging In to OneAccess and Accessing Applications

Account Settings

3.1 Logging In to OneAccess and Accessing Applications

This section describes how to log in to the user portal and access different applications.

Prerequisites

You have a user account for the OneAccess user portal. If you do not have a user account, contact your enterprise administrator to create one for you.

Procedure

Log in to the user portal through username+password, OTP, SMS, or WeLink authentication. If the authentication is successful, the user portal homepage is displayed.

Step 1 Go to the user portal login page.

NOTE

Obtain the user portal URL from the enterprise administrator. For example, **https://example.huaweicloudoneaccess.com**.

Step 2 Enter your account information and click **Log In**.

Step 3 On the user portal homepage, click the application you want to access.

----End

 Copyright © Huawei Technologies Co., Ltd.

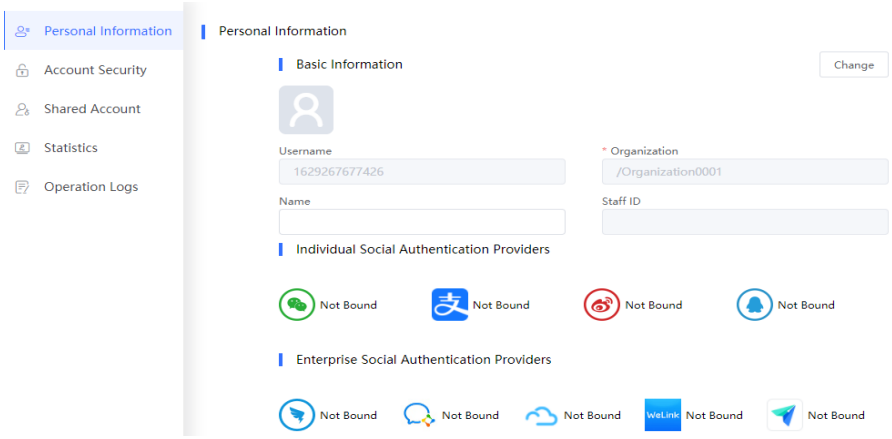
3.2 Account Settings

In the user portal, view and modify your personal information and configure account security settings.

Viewing and Modifying Personal Information

Go to the **Account Settings** page, choose **Personal Information** in the left pane, and view and modify your personal information.

Figure 3-1 Personal Information



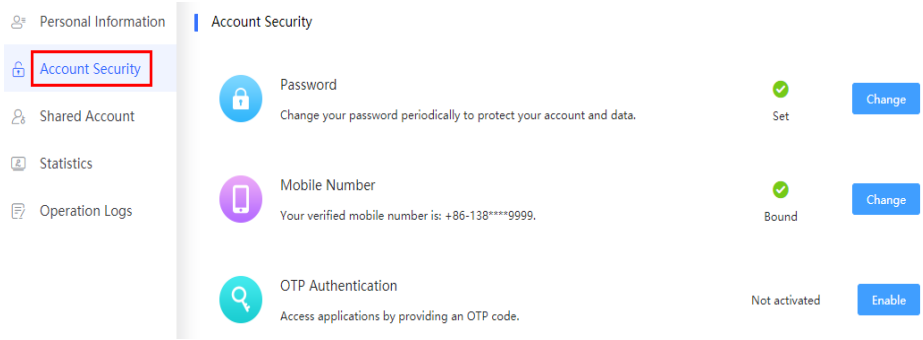
NOTE

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.

Account Security

Go to the **Account Settings** page, choose **Account Security** in the left pane, change your login password and mobile number, and enable OTP authentication.

Figure 3-2 Account Security



- **Password**: Change the login password of your account.

 Copyright © Huawei Technologies Co., Ltd.

- **Mobile Number**: Change the mobile number associated with your account.
- OTP Authentication

  An OTP is generated by a virtual MFA device in compliance with the TOTP standard.

  – Binding a virtual MFA device

    Install an MFA application (an authenticator) on your mobile phone and bind it to your account.

    i. Go to the **Account Settings** page, and choose **Account Security** in the left pane.

    ii. Click **Enable** on the right of **OTP Authentication**.

    iii. Add your account to an MFA application as instructed.

      ○ Scan the QR code

        Open the MFA application on your mobile phone, and use the MFA application to scan the QR code displayed on the **Enable OTP Authentication** page.

      ○ Enter the secret key

        Open the MFA application on your mobile phone, and enter your username and secret key in the MFA application.

        NOTE

        To ensure that you can perform MFA-based verification successfully, confirm that you have enabled the automatic time setup option on your mobile phone.

    iv. On the **Enable OTP Authentication** page, enter an OTP (that is, an MFA verification code) obtained from the MFA application, and click **OK**.

  – Obtaining a virtual MFA verification code

    If the enterprise administrator has enabled login authentication or MFA authentication, after you bind a virtual MFA device to your account, you need to enter an MFA verification code during login. Open the MFA application on your smart device, view the verification code displayed next to your user account, and enter the code on the login page.

  – Resetting the virtual MFA device

    To reset the virtual MFA device bound to your account, do as follows:

    i. Click **Reset** on the right of **OTP Authentication**.

    ii. On the **Reset OTP** page, click **Send SMS code**.

    iii. Enter the verification code sent to your mobile phone and click **Next**.

    iv. Bind a new virtual MFA device to your account. For details, see **Binding a virtual MFA device**.

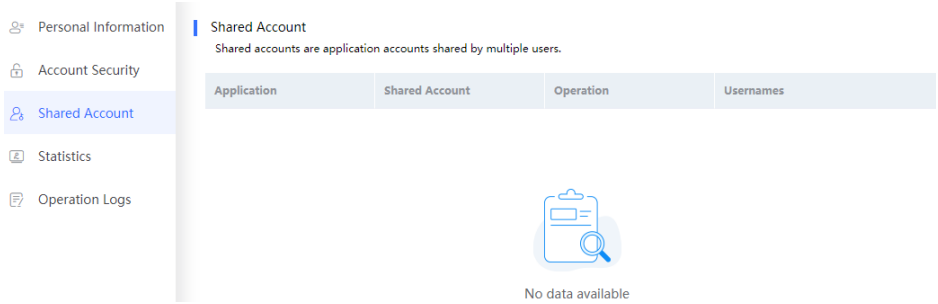
Managing Shared Accounts

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 **Modifying Application Configurations**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-3 Shared Accounts



Statistics

Go to the **Account Settings** page, choose **Statistics** in the left pane, and view your frequently accessed applications, frequent locations, authentication statistics, frequently used authentication types, authentication failure causes, and frequently used devices.

Operation Logs

Go to the **Account Settings** page, choose **Operation Logs** in the left pane, and view your operation logs. Query operation logs by time, operation type, client type, or operation result.

 Copyright © Huawei Technologies Co., Ltd.

4 Change History

Table 4-1 Change history

Released On	Description
2021-08-17	This issue is the fourth official release, in which some chapters are optimized.
2021-06-24	This issue is the third official release, which incorporates the following changes: • Added descriptions about calling built-in APIs in **Calling Built-in APIs**. • Added section **CloudBridge Agent Configuration**.
2021-05-15	This issue is the second official release, which incorporates the following changes: • Optimized the document content and added screenshots. • Added section **Voice Gateway**. • Added section **DingTalk Gateway**. • Added section **Importing Shared Accounts**. • Added section **Managing Shared Accounts**.
2021-01-13	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.