Best Practices

Best Practices

Issue 01

Date 2021-08-31



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 Identity Source Integration 1
1.1 Integrating AD 1
1.2 Integrating LDAP 6
2 Application Integration 13
2.1 SSO Access to Applications Through SAML 13
2.2 SSO Access to Applications Through OAuth2.0 22
2.3 SSO Access to Applications Through OIDC 29
2.4 SSO Access to Applications Through CAS 35
3 Data Synchronization 42
3.1 Synchronizing Data to Atlassian Through SCIM 42
3.2 Synchronizing Data Through LDAP 48
4 Authentication Provider Integration 57
4.1 SAML Authentication 57
4.2 OIDC Authentication 64
4.3 CAS Authentication 74
4.4 OAuth Authentication 80
4.5 AD Authentication 88
4.6 LDAP Authentication 98
4.7 Kerberos Authentication 109
4.8 eteams Authentication 115
5 Interconnection with HUAWEI CLOUD 120
5.1 SSO Access to HUAWEI CLOUD 120
6 Authorizing IAM Users to Access a OneAccess Instance 128
7 Voice Gateway Configuration 134
8 Email Gateway Configuration 137

 Copyright © Huawei Technologies Co., Ltd.

1 Identity Source Integration

Integrating AD

Integrating LDAP

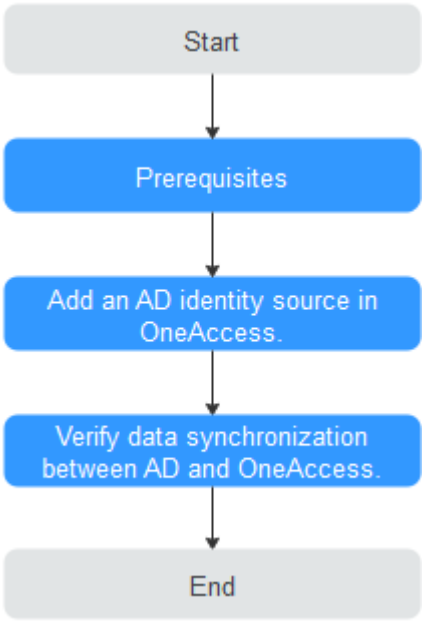
1.1 Integrating AD

OneAccess allows you to import user and organization information from identity sources and synchronize the information with them in real time.

This section describes how to integrate Active Directory (AD) with OneAccess. AD is a directory service developed by Microsoft for Windows domain networks. It provides single sign-on (SSO) and multi-factor authentication (MFA) to help protect users from cybersecurity attacks.

Configuration Process

Figure 1-1 Configuration process



 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- You have administrator permissions for the AD platform in your enterprise.
- You have permissions to access the administrator portal.
- Your AD platform can be connected to the OneAccess administrator portal.
- You know how to obtain parameters of the AD platform and how to use this platform.

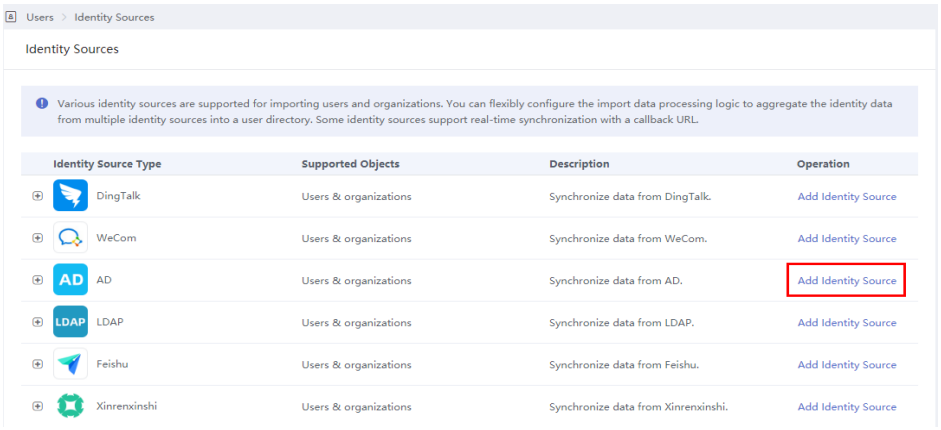
Adding an AD Identity Source in OneAccess

Configure parameters of the AD identity source so that OneAccess can synchronize data from it.

Step 1 Add an identity source in OneAccess.

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

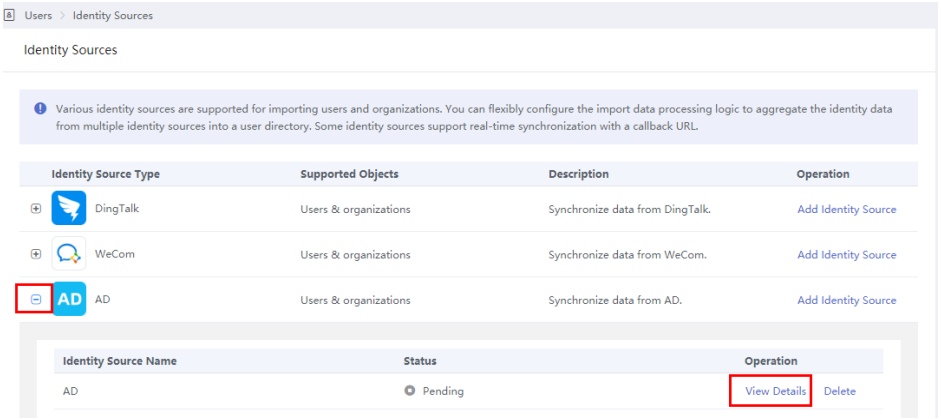
Figure 1-2 Adding an AD identity source



Step 2 Configure import settings.

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

Figure 1-3 Viewing details of an AD identity source



 Copyright © Huawei Technologies Co., Ltd.

2. Click the **Import Settings** tab, set import parameters, and click **Save**.
   - **Basic Settings**: Connection parameters of your AD server to be connected to OneAccess.
   - **Optional Settings**: Whether to synchronize passwords, password attributes to be synchronized, and account and organization object classes. Modify these settings if a synchronization error occurs. For certain parameters, you may retain the default values.
   - **Advanced Settings**: Policies for mapping top-level organizations, organizations, and users.

Table 1-1 Basic parameters

Parameter	Description
* Host	Host name or IP address of the AD server.
TCP Port	TCP/IP port of the AD server. The default port is 389. **NOTE** OneAccess can be accessed only over public networks. Provide the public network address of your server and enable port 389.
SSL	Default value: **true**, which indicates that SSL is used to connect the AD server.
Protocol Version	Default value: **TLSv1.2**; recommended: **TLSv1.3** and **TLSv1.2**.
Principal	Identifier used for AD server authentication. Specify an account that has read permission for the AD domain. The input parameter will contain the domain name, for example, **admin@test.com** and **TEST\admin**.
Password	Password of the account.
* Base Contexts	One or more top-level nodes (for example, **OU=huaweitest,DC=test,DC=com**) in the AD tree to be considered as the beginning for synchronizing AD accounts.

Table 1-2 Advanced settings

Parameter	Description
Scheduled Synchronization	Time for scheduled synchronization every day.
Organization	Parent organization in OneAccess to which organizations will be synchronized from AD. A new top-level organization will be automatically created if this parameter is not set.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Deletion Threshold	A protection mechanism provided by OneAccess. Default value: **100**. If OneAccess is notified that data exceeding the threshold was deleted in the AD, OneAccess will only delete data within the threshold and retain the excessive data.
Organization Matching	Organization mapping rules for OneAccess to synchronize organization data from your AD. For example, OneAccess has an organization attribute **Code** and your AD has a similar attribute **Organization Code**. Organizations in your AD will be mapped to OneAccess, and their codes in the AD will be identified as organization codes in OneAccess.
Create Organization	Enabled by default, indicating that OneAccess will automatically create organizations that do not match any organizations in OneAccess. To ensure data integrity, keep this option enabled.
Update Organization	Enabled by default, indicating that organizations in OneAccess that match those synchronized from the identity source will be updated. To ensure data accuracy, keep this option enabled.
Delete Organization	Indicates whether to delete organizations in OneAccess if the corresponding organizations in your AD are deleted. By default, **Retain** is selected. ▪ **Retain**: OneAccess retains all organizations that are successfully synchronized. ▪ **Delete**: OneAccess deletes organizations according to changes in your AD.
User Matching	User mapping rules for OneAccess to synchronize user data from your AD. For example, OneAccess has a user attribute **User ID** and your AD has a similar attribute **Employee ID**. Users in your AD will be mapped to OneAccess, and their employee IDs in the AD will be identified as user IDs in OneAccess.
Create User	Enabled by default, indicating that OneAccess will automatically create users that do not match any users in OneAccess. To ensure data integrity, enable this option.
Update User	Enabled by default, indicating that users in OneAccess that match those synchronized from the identity source will be updated. To ensure data accuracy, keep this option enabled.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Delete User	Indicates whether to delete users in OneAccess if the corresponding users in your AD are deleted. By default, **Deactivate** is selected. ▪ **Deactivate**: OneAccess deactivates users deleted in your AD. ▪ **Retain**: OneAccess retains users deleted in your AD. ▪ **Delete**: OneAccess deletes users deleted in your AD.

Step 3 (Optional) Set the object models.

Click the **Object Models** tab. Then add, modify, or delete user and organization attributes and mapping rules.

Table 1-3 Object model parameters

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

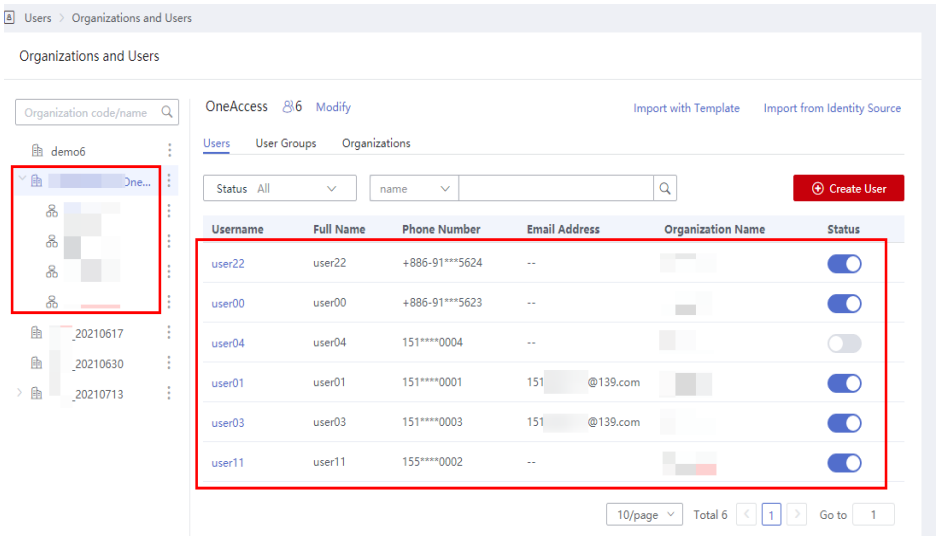
----End

Verifying Synchronization of AD Data

- Manual synchronization: Go to the AD identity source details page, click the **Synchronization** tab, and click **Execute**. OneAccess synchronizes user and organization data from the AD identity source, and generates operation records.
  - Click **View Details** in the row that contains the target record to view details.
  - View the synchronized users and organizations on the **Organizations and Users** page.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-4 Viewing synchronized data



- Scheduled synchronization: If you have configured the time for scheduled synchronization in the **Advanced Settings** section of the **Import Settings** tab page, view the records on the **Scheduled Synchronization** page.

1.2 Integrating LDAP

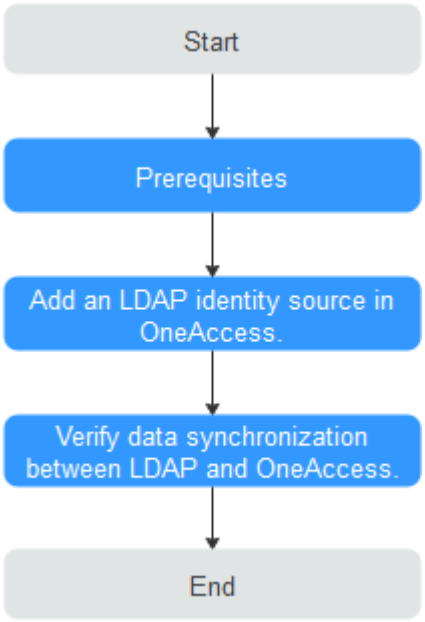
OneAccess allows you to import user and organization information from identity sources and synchronize the information with the identity sources in real time.

This section describes how to integrate a Lightweight Directory Access Protocol (LDAP) identity source with OneAccess. LDAP is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It is often used for authentication and storing information about users, groups, and applications.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process

Figure 1-5 Configuration process



Prerequisites

- You have administrator permissions for the LDAP platform in your enterprise.
- You have permissions to access the administrator portal.
- Your LDAP platform can be connected to the OneAccess administrator portal.
- You are familiar with the LDAP protocol and know how to obtain information about your LDAP server.

Adding an LDAP Identity Source in OneAccess

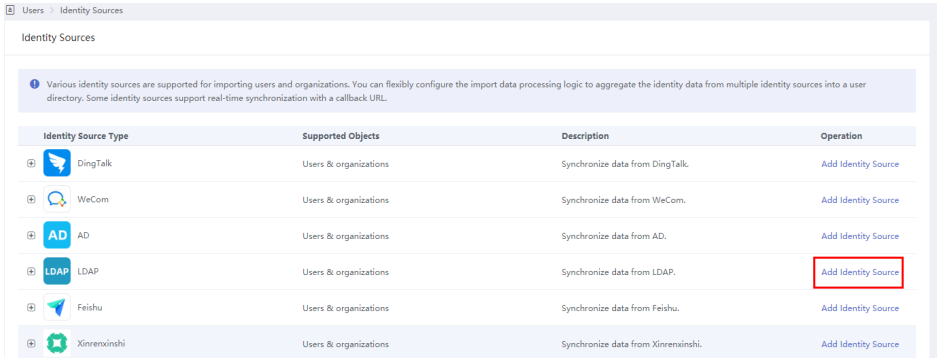
Configure parameters of the LDAP identity source in OneAccess to ensure that OneAccess can synchronize data from your LDAP server.

Step 1 Add an identity source in OneAccess.

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

 Copyright © Huawei Technologies Co., Ltd.

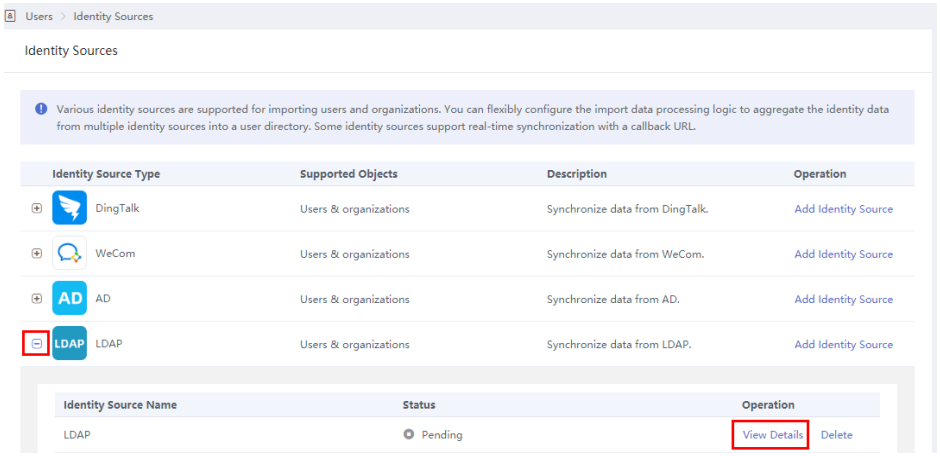
Figure 1-6 Adding an LDAP identity source



Step 2 Configure import settings.

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

Figure 1-7 Viewing details of an LDAP identity source



2. Click the **Import Settings** tab, set import parameters, and click **Save**.
   - **Basic Settings**: Connection parameters of your LDAP server to be connected to OneAccess.
   - **Optional Settings**: Whether to synchronize passwords, password attributes to be synchronized, and account and organization object classes. Modify these settings if a synchronization error occurs. For certain parameters, you may retain the default values.
   - **Advanced Settings**: Policies for mapping top-level organizations, organizations, and users.

Table 1-4 Basic parameters

Parameter	Description
* Host	Host name or IP address of the LDAP server.
TCP Port	TCP/IP port of the LDAP server. The default port is 389. **NOTE** OneAccess can be accessed only over public networks. Provide the public network address of your LDAP server and enable port 389.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
SSL	Default value: **true**, which indicates that SSL is used to connect the LDAP server.
Protocol Version	Default value: **TLSv1.2**; recommended: **TLSv1.3** and **TLSv1.2**.
Principal	Account name used for LDAP server authentication. The input parameter will contain the domain name, for example, **admin@test.com** and **TEST\admin**.
Password	Password of the account.
* Base Contexts	One or more top-level nodes in the LDAP tree to be considered as the beginning for synchronizing data. Searching for specific users or user groups in the LDAP server will start from these nodes. For example, **OU=huaweitest,DC=test,DC=com**.

Table 1-5 Advanced settings

Parameter	Description
Scheduled Synchronization	Time for scheduled synchronization every day.
Organization	Parent organization in OneAccess to which organizations will be synchronized from your LDAP server. A new top-level organization will be automatically created if this parameter is not set.
Deletion Threshold	A protection mechanism provided by OneAccess. Default value: **100**. If OneAccess is notified that data exceeding the threshold was deleted in your LDAP server, OneAccess will only delete data within the threshold and retain the excessive data.
Organization Matching	Organization mapping rules for OneAccess to synchronize organization data from your LDAP server. For example, OneAccess has an organization attribute **Code** and your AD has a similar attribute **Organization Code**. Organizations in your LDAP will be mapped to OneAccess, and their codes in the LDAP will be identified as organization codes in OneAccess.
Create Organization	Enabled by default, indicating that OneAccess will automatically create organizations that do not match any organizations in OneAccess. To ensure data integrity, enable this option.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Update Organization	Enabled by default, indicating that organizations in OneAccess that match those synchronized from the identity source will be updated. To ensure data accuracy, keep this option enabled.
Delete Organization	Indicates whether to delete organizations in OneAccess if the corresponding organizations in your LDAP server are deleted. By default, **Retain** is selected. – **Retain**: OneAccess retains all organizations that are successfully synchronized. – **Delete**: OneAccess deletes organizations according to changes in your LDAP server.
User Matching	User mapping rules for OneAccess to synchronize user data from your LDAP server. For example, OneAccess has a user attribute **User ID** and your LDAP has a similar attribute **Employee ID**. Users in your LDAP will be mapped to OneAccess, and their employee IDs in the LDAP will be identified as user IDs in OneAccess.
Create User	Enabled by default, indicating that OneAccess will automatically create users that do not match any users in OneAccess. To ensure data integrity, enable this option.
Update User	Enabled by default, indicating that users in OneAccess that match those synchronized from the identity source will be updated. To ensure data accuracy, keep this option enabled.
Delete User	Indicates whether to delete users in OneAccess if the corresponding users in your LDAP server are deleted. By default, **Deactivate** is selected. – **Deactivate**: OneAccess deactivates users deleted in your LDAP server. – **Retain**: OneAccess retains users deleted in your LDAP server. – **Delete**: OneAccess deletes users deleted in your LDAP server.

Step 3 (Optional) Set the object models.

Click the **Object Models** tab. Then add, modify, or delete user and organization attributes and mapping rules.

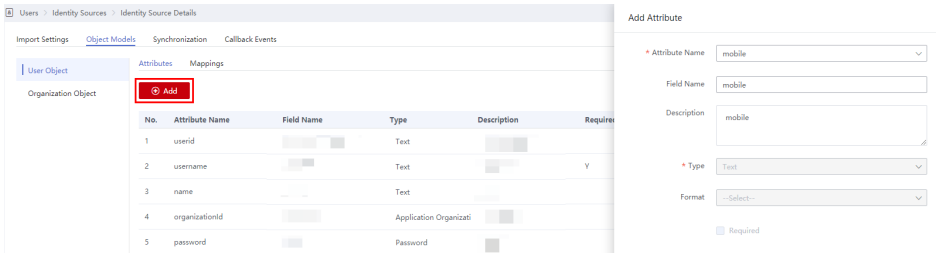
Table 1-6 Object model parameters

Parameter		Description
User Object	Attributes	User attributes in the LDAP identity source.

 Copyright © Huawei Technologies Co., Ltd.

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

Figure 1-8 Defining user attributes

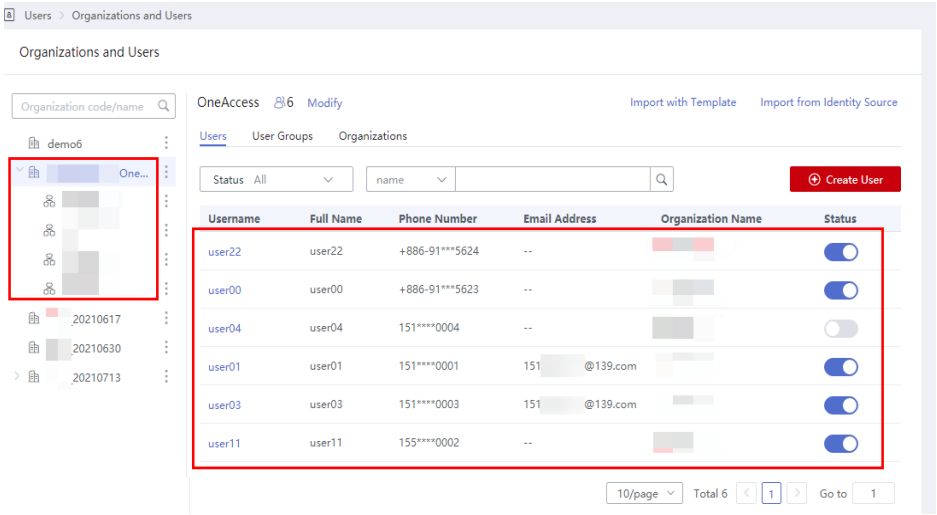


----End

Verifying Synchronization of LDAP Data

- Manual synchronization: Go to the LDAP identity source details page, click the **Synchronization** tab, and click **Execute**. OneAccess synchronizes user and organization data from the LDAP identity source, and generates operation records.
  - Click **View Details** in the row that contains the target record to view details.
  - View the synchronized users and organizations on the **Organizations and Users** page.

Figure 1-9 Viewing synchronized data



 Copyright © Huawei Technologies Co., Ltd.

- Scheduled synchronization: If you have configured the time for scheduled synchronization in the **Advanced Settings** section of the **Import Settings** tab page, view the records on the **Scheduled Synchronization** page.

 Copyright © Huawei Technologies Co., Ltd.

2 Application Integration

SSO Access to Applications Through SAML

SSO Access to Applications Through OAuth2.0

SSO Access to Applications Through OIDC

SSO Access to Applications Through CAS

2.1 SSO Access to Applications Through SAML

Introduction

Security Assertion Markup Language (SAML), developed by the Security Services Technical Committee of OASIS, is an open-source standard data format based on XML. SAML exchanges authentication and authorization data between different security domains, meeting the SSO requirements of web applications.

Learn about the following **terms** and **authorization process** related to SAML.

- Terms

  Table 2-1 Terms

Term	Description
IdP	Identity provider (IdP), which collects and stores user identity information, such as usernames and passwords, and authenticates users during login.
SP	Service provider (SP), which establishes a trust relationship with an IdP and uses the user information provided by the IdP to provide services.
SSO	Single sign-on, a process in which users can access a trusted service provider (SP) through a specific redirect URL in OneAccess.

- Authorization process

 Copyright © Huawei Technologies Co., Ltd.

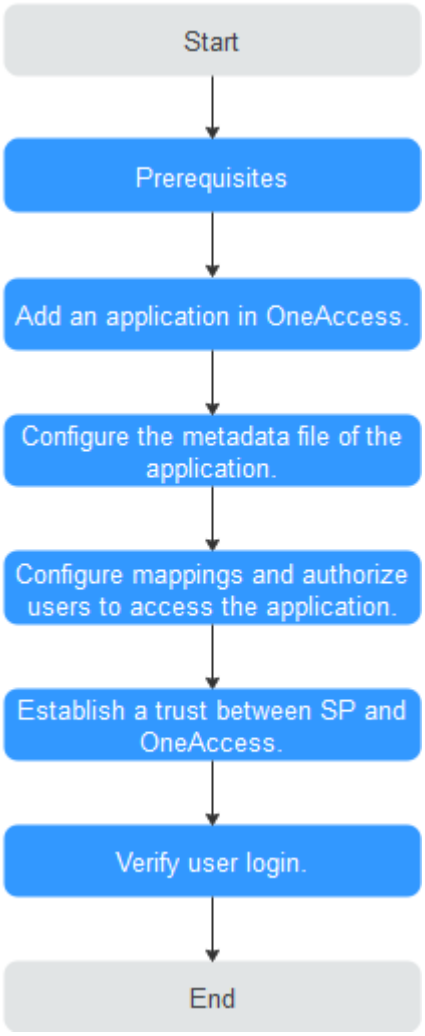
a. A user accesses a web application using a browser.
b. The web application generates a SAML authentication request.
c. The web application sends the redirect URL to the user's browser. The redirect URL contains the encoded SAML authentication request, which should be submitted to the SSO service.
d. The IdP decodes the SAML request.
e. The IdP authenticates the user. If the authentication is successful, the IdP generates a SAML response, encodes it, and then returns it to the user's browser. The response contains the user's username.
f. The browser forwards the SAML response to the assertion consumer service (ACS) URL of the web application.
g. The web application uses the public key of the IdP to verify the SAML response. If the verification is successful, ACS redirects the user to the target URL.
h. The user is redirected to the target URL and logged in to the web application.

This section describes how to integrate an application with OneAccess using the SAML protocol.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process

Figure 2-1 Configuration process



Prerequisites

You have permissions to access the administrator portal.

Adding an Application

Add an application in the administrator portal, and configure the application's metadata file to establish a trust. The application serves as an SP.

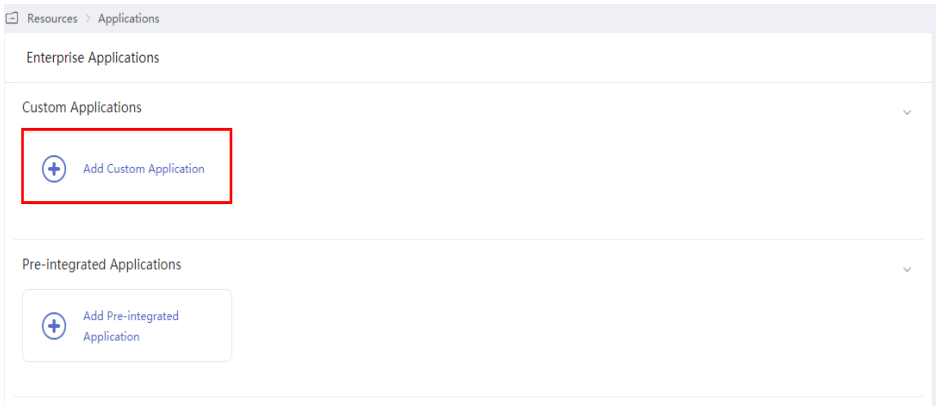
Step 1 Log in to the administrator portal.

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

Step 3 Click **Add Custom Application** in the **Custom Applications** section, set the logo and application name, and click **Save**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 Adding a custom application



----End

Configuring a Metadata File

Upload the metadata file of the SP or manually configure the metadata. If the metadata has changed, update it so that users can log in to the application through OneAccess.

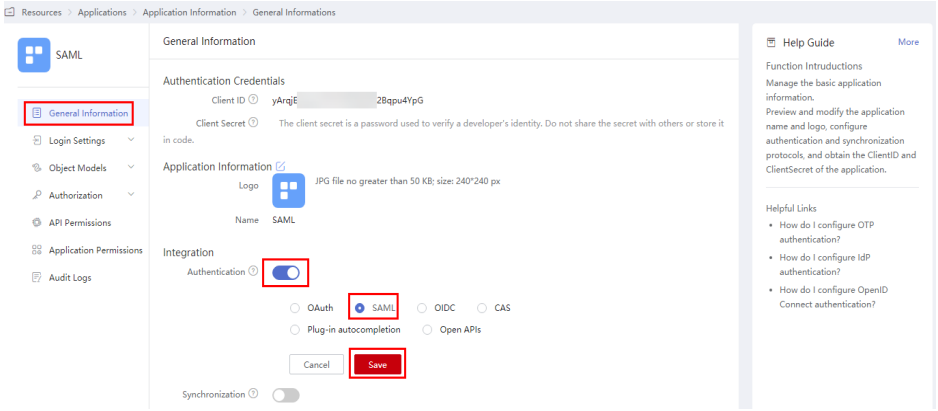
Step 1 Click the application added in **Adding an Application** and click the application icon on the application information page.

Step 2 On the application details page, choose **General Information** > **Integration**, enable authentication, select **SAML**, and click **Save**.

NOTE

The protocol cannot be changed once specified.

Figure 2-3 Selecting an authentication protocol



Step 3 Click **Authentication Settings** in the left pane, and **upload a metadata file** or **manually edit the metadata**.

 Copyright © Huawei Technologies Co., Ltd.

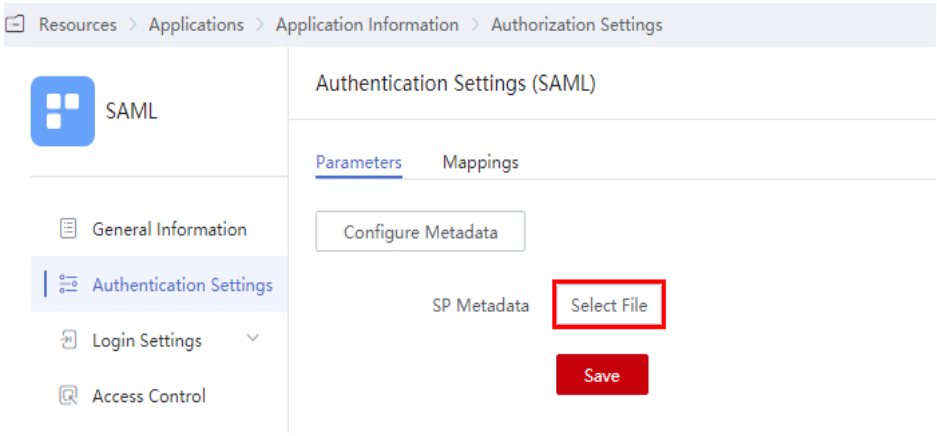
CAUTION

To avoid information leakage, do not include sensitive information in the configuration parameters.

----End

- Upload a metadata file
  a. On the **Authentication Settings** page, click **Import SP Metadata**.
  b. Click **Select File** and select the metadata file of the SP.

  Figure 2-4 Uploading a metadata file



  c. When the **Select File** button changes to √, the system has extracted the metadata. Click **Save**.

  NOTE

  - If a message indicating incorrect file type is displayed, upload the correct metadata file or edit the metadata.
  - For details about how to obtain the metadata of the application, see the application's documentation.

- Edit metadata
  a. Click **Configure Metadata**.
  b. Set the required parameters according to the metadata file of the application.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-5 Configuring authentication parameters

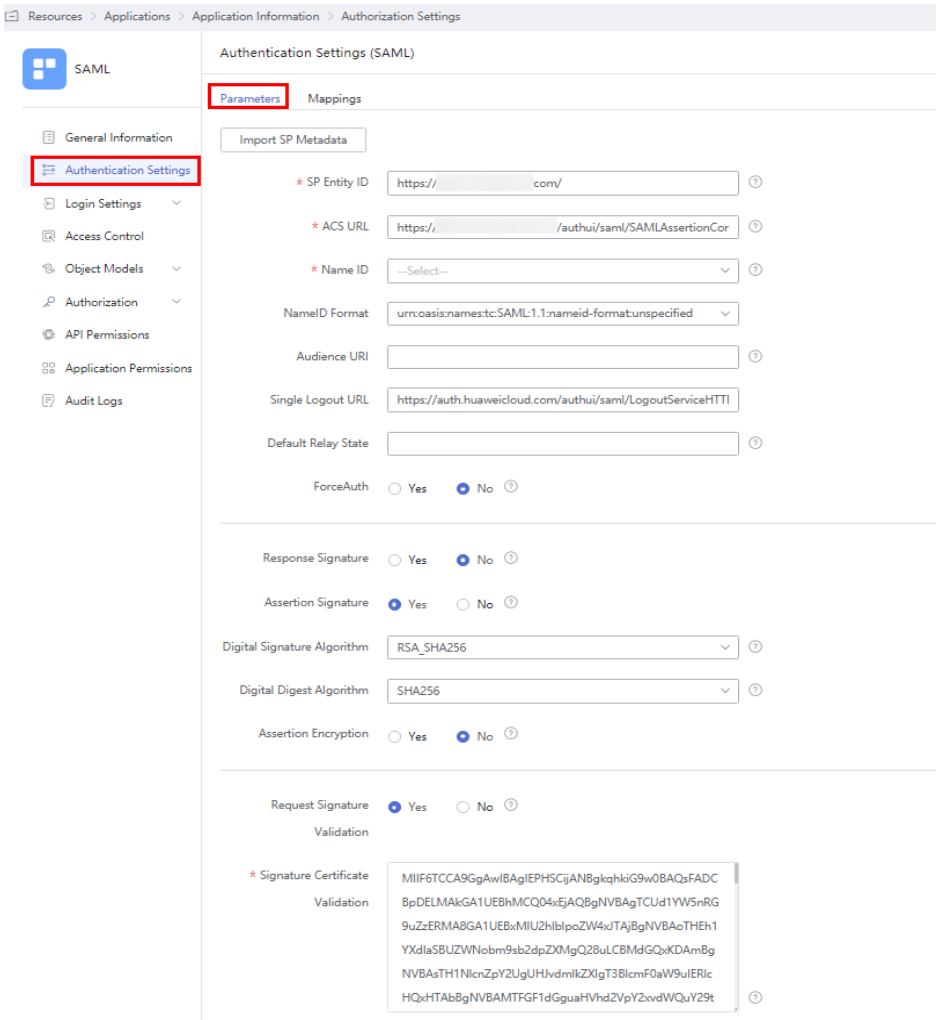


Table 2-2 Authentication parameters

Parameter	Mandatory	Description
SP Entity ID	Yes	Unique identifier of the 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
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 in OneAccess.
Default Relay State	No	URL to which users will be redirected after successful login.
ForceAuth	Yes	Disabled by default. If this option is enabled, users will be authenticated again as required by the SP.
Response Signature	Yes	Disabled by default. This option indicates whether to sign SAML responses using the IdP's certificate.
Assertion Signature	Yes	Disabled by default. This option indicates whether to sign assertions using the IdP's certificate. Enter the value of **WantAssertionsSigned** displayed in the SP metadata file.
Digital Signature Algorithm	Yes	Algorithm used to sign SAML responses or assertions. By default, **RSA_SHA256** is used.
Digital Digest Algorithm	Yes	Algorithm used to create digests for SAML responses or assertions. By default, **SHA256** is used.
Assertion Encryption	Yes	Disabled by default. This option indicates whether to encrypt assertions.
Request Signature Validation	Yes	Enabled by default. This option indicates whether to sign SAML requests. Enter the value of **AuthnRequestsSigned** displayed in the SP metadata file.
Signature Certificate Validation	Yes	SP public key certificate, which is used to verify SAML request signatures. Enter the content of **use="signing"** displayed in the SP metadata file.

Configuring Mappings and Authorizing Users

Configure attributes that need to be returned to the application after successful authentication.

Then authorize specific users to access the application.

 Copyright © Huawei Technologies Co., Ltd.

- Mapping configuration

  NOTE

  If you have configured the required mapping using **Name ID** in **Configuring a Metadata File**, skip this step.

  a. On the **Authentication Settings** page, click the **Mappings** tab, and click **Add Mapping** to add an attribute mapping.

  Figure 2-6 Adding a mapping

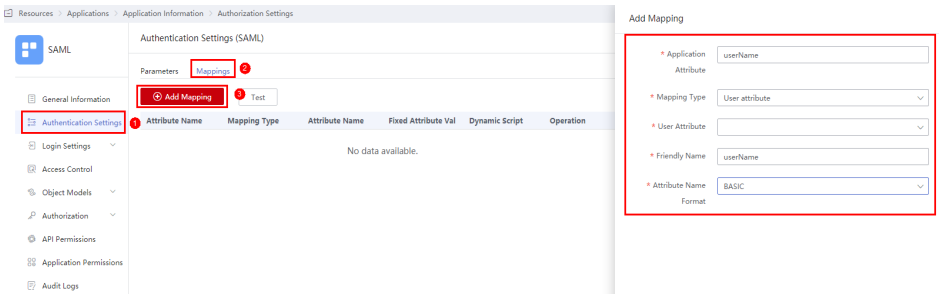


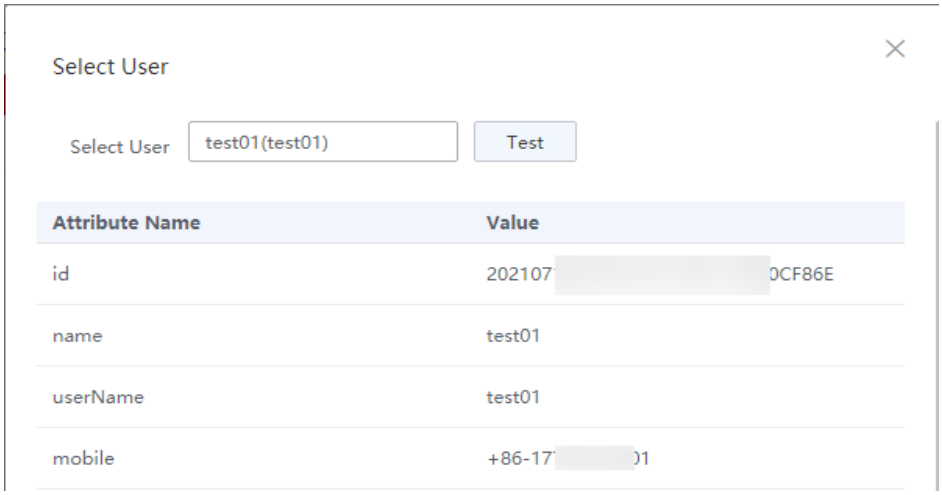
  Table 2-3 Mapping parameters

Parameter	Description
Application Attribute	(Required) User attribute that OneAccess will return to the application after successful authentication.
Mapping Type	(Required) The mapping type determines the returned attribute value.
User Attribute	(Required) Attribute mapped from OneAccess to the application.
Friendly Name	(Required) Enter the same value as the **Application Attribute**.
Attr Name Format	(Required) Format of data returned in accordance with the SAML protocol.

  b. Click **Test**. On the **Select User** page, enter a username to test the mappings.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-7 Testing mappings



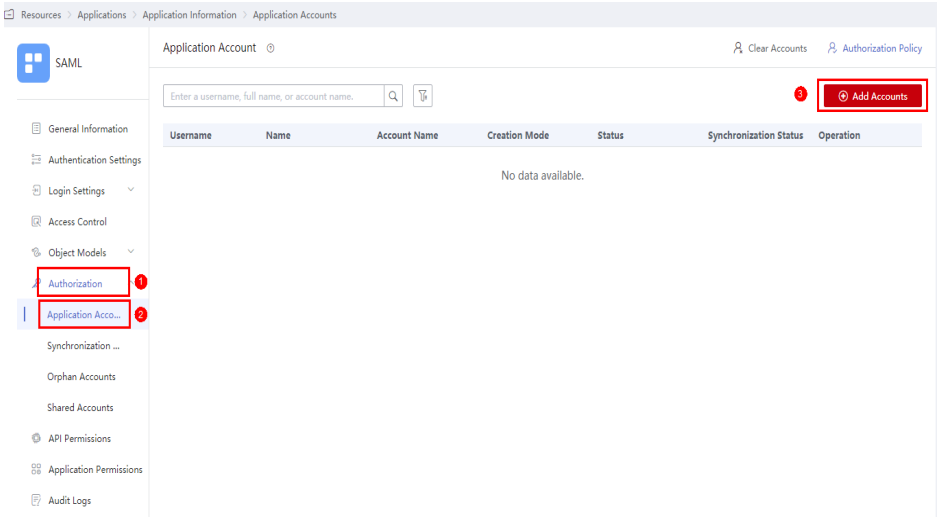
- User authorization

  In the left pane, choose **Authorization** > **Application Accounts**. Then click **Add Accounts** to authorize specific users to access the application. To authorize access using a policy, see the descriptions about the application account authorization policy in **Modifying Application Configurations**.

  NOTE

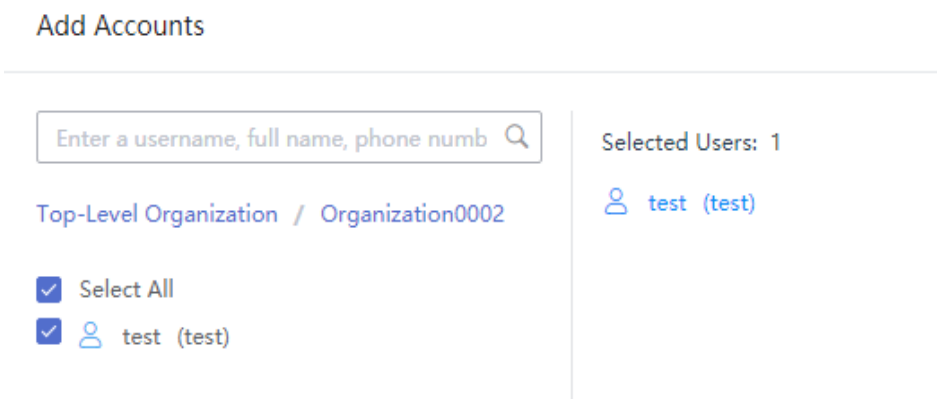
  For details about how to configure login, access control, and object models, see **Modifying Application Configurations**.

Figure 2-8 Adding accounts



 Copyright © Huawei Technologies Co., Ltd.

Figure 2-9 Selecting users



Establishing a Trust Between the SP and OneAccess

Configure the metadata file of OneAccess in the SP server to establish a trust on OneAccess.

Step 1 Download the metadata file of OneAccess.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Settings** > **Server Settings**. Then click **IdP**.
3. On the **IdP** page, click **Download IdP Metadata** in the upper right. The metadata file is automatically saved.

Step 2 Upload the metadata file to the SP server. For details, see the SP's documentation.

Step 3 Obtain the metadata file of the SP. For details, see the SP's documentation.

----End

Logging In as a User

Log in to the user portal as one of the **authorized users**, and click the target application to check whether you can access it.

2.2 SSO Access to Applications Through OAuth2.0

Introduction

Open Authorization (OAuth) is an open standard that allows users to authorize third-party applications to access their information stored on a specific resource server without sharing usernames and passwords with the applications.

1. When a user accesses a third-party application, the application sends an authorization request to OneAccess. If the user agrees to authorize the application, OneAccess redirects the user to the application with an authorization code.
2. The application uses the authorization code to invoke OneAccess' API to obtain an access token.

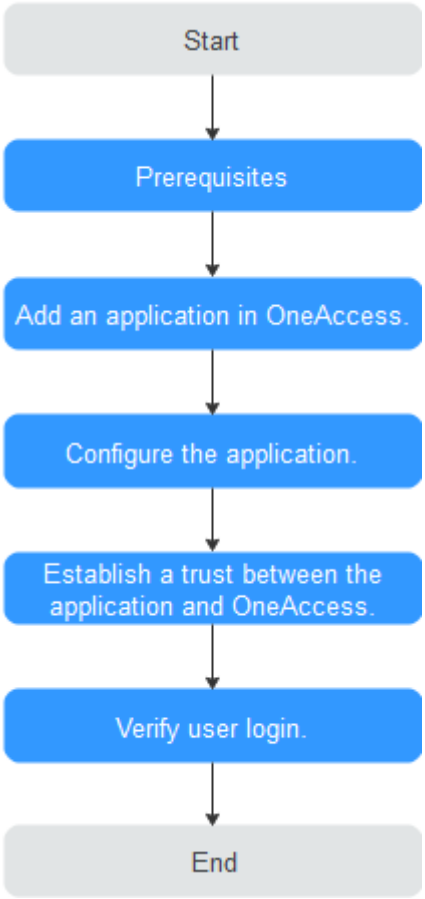
 Copyright © Huawei Technologies Co., Ltd.

3. The application uses the obtained access token to invoke other APIs of OneAccess to obtain user information. The token must be valid.

This section describes how to integrate an application with OneAccess using the OAuth protocol.

Configuration Process

Figure 2-10 Configuration process



Prerequisites

You have permissions to access the administrator portal.

Adding an Application

Add an application in the administrator portal, and configure authentication information to establish a trust on it.

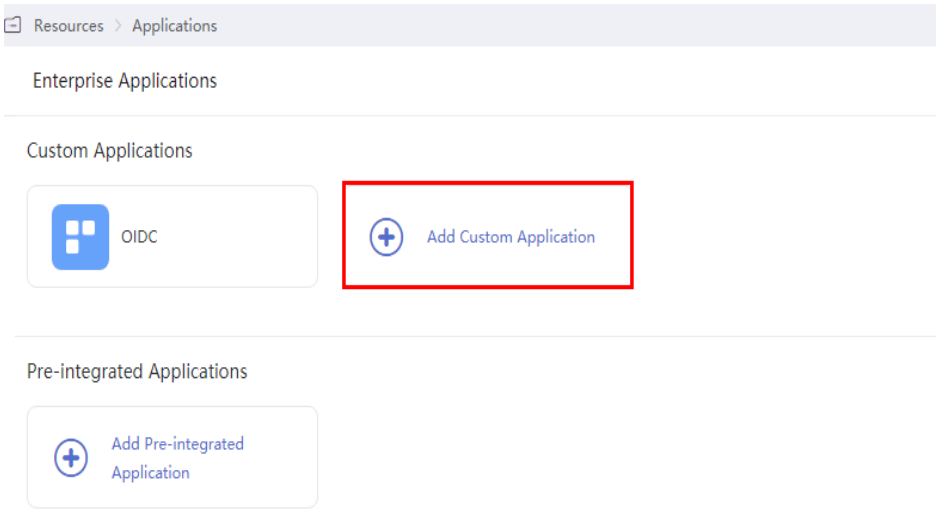
Step 1 Log in to the administrator portal.

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

Step 3 Click **Add Custom Application** in the **Custom Applications** section, set the logo and application name, and click **Save**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-11 Adding a custom application



----End

Configuring the Application

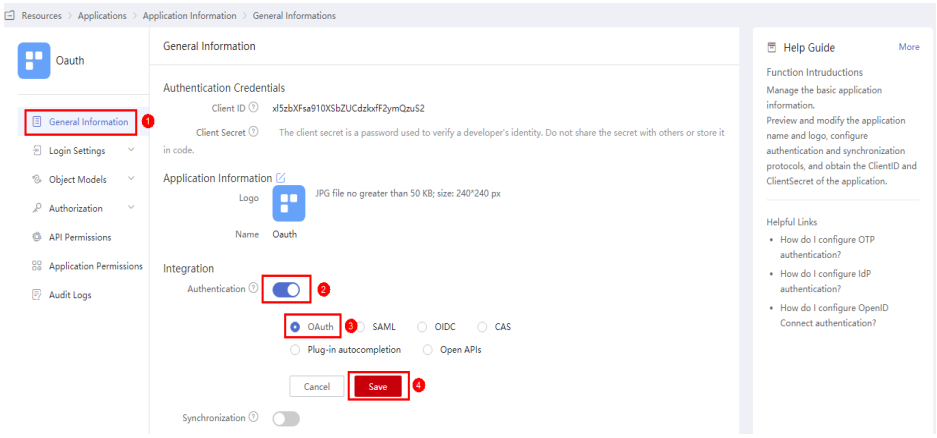
Configure the application in OneAccess so that users can log in to it through OneAccess. For details, see **authentication configuration**, **mapping configuration (optional)**, and **user authorization**.

- Authentication configuration
  a. Click the application added in **Adding an Application** and click the application icon on the application information page.
  b. On the application details page, choose **General Information** > **Integration**, enable authentication, select **OAuth**, and click **Save**.

  NOTE

  The protocol cannot be changed once specified.

  Figure 2-12 Selecting an authentication protocol

  c. Click **Authentication Settings** in the left pane, and configure the authentication parameters.

CAUTION

To avoid information leakage, do not include sensitive information in the configuration parameters.

Figure 2-13 Configuring authentication parameters

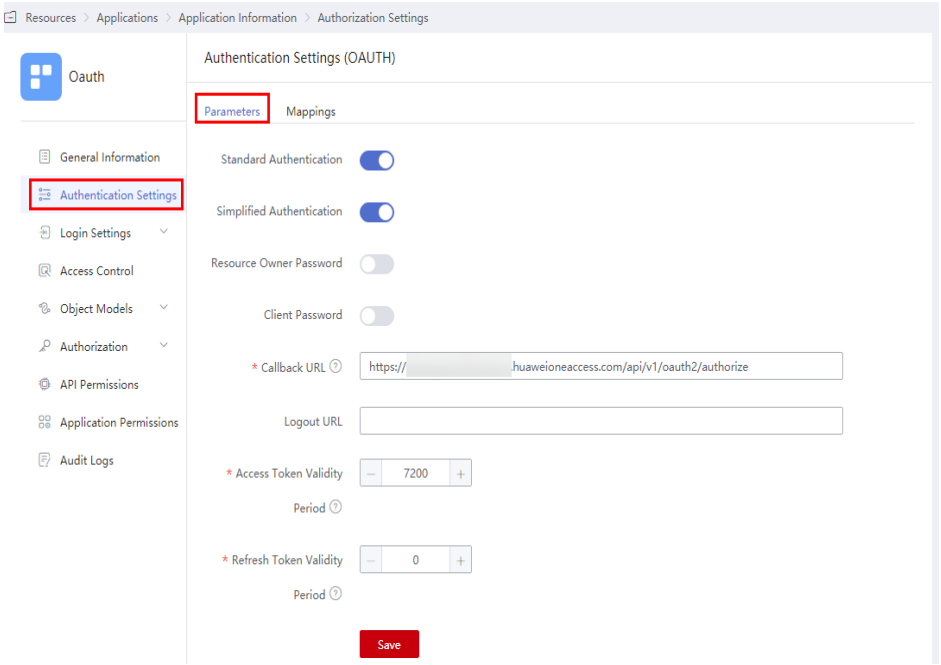


Table 2-4 Authentication parameters

Parameter	Description
Standard Authentication	Enabled by default. It is the most widely used and most secure authentication mode, and is suitable for web applications that have backends. In this mode, the authorization code is transferred at the frontend, and the token is stored at the backend to prevent leakage. All communications with the resource server are completed at the backend. For details about the standard authorization mode, see **Introduction**.
Simplified Authentication	Disabled by default. It is suitable for web applications that do not have backends and must store tokens at the frontend in low security scenarios. Different from the standard authorization mode, this mode does not involve authorization codes.
Resource Owner Password	Disabled by default. This mode is suitable for scenarios where users have high trust in clients. Users provide their usernames and passwords to the clients to apply for tokens.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Client Password	Disabled by default. This mode is suitable for applications that do not have frontends. In this mode, clients initiate token requests.
Callback URL	(Required) Callback URL to be visited after successful authorization. Enter a trusted domain name, and separate multiple domain names using commas (,) if any. The application homepage is recommended, for example, **https://xxx.xxx.xxx.com**.
Logout URL	(Optional) Logout URL to be visited after a user logs out of their session.
Access Token Validity Period	Validity period of the access token in seconds. The default value is 7200 seconds, that is, 2 hours.
Refresh Token Validity Period	Validity period of the refresh token. The default value is **0**, indicating that the refresh token is not supported. When the access token of a user expires, the user can use their refresh token to obtain a new one. **NOTE** The prerequisite for automatic token update is that the validity period of the refresh token is longer than that of the access token.

- (Optional) Mapping configuration
  a. On the **Authentication Settings** page, click the **Mappings** tab, and click **Add Mapping** to add an attribute mapping.

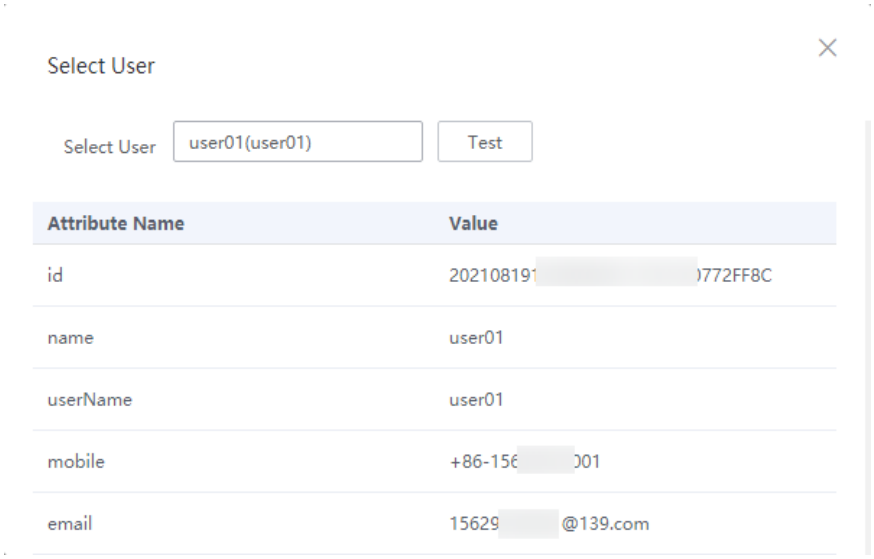
  Table 2-5 Mapping parameters

Parameter	Description
Application Attribute	(Required) User attribute that OneAccess will return to the application after successful authentication.
Mapping Type	(Required) The mapping type determines the returned attribute value.
User Attribute	(Required) Attribute mapped from OneAccess to the application.

  b. Click **Test**. On the **Select User** page, enter a username to test the mappings.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-14 Testing mappings



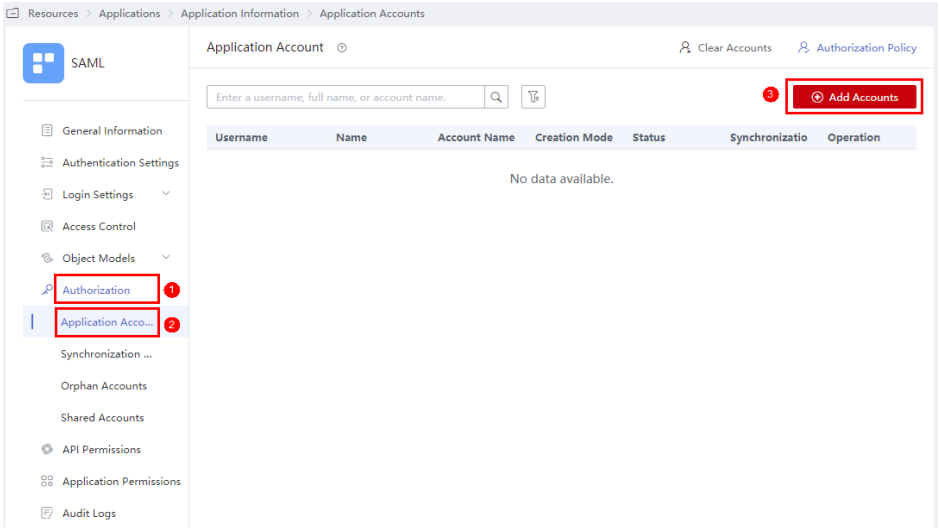
- User authorization

  In the left pane, choose **Authorization** > **Application Accounts**. Then click **Add Accounts** to authorize specific users to access the application. To authorize access using a policy, see the descriptions about modifying application permissions in **Modifying Application Configurations**.

  NOTE

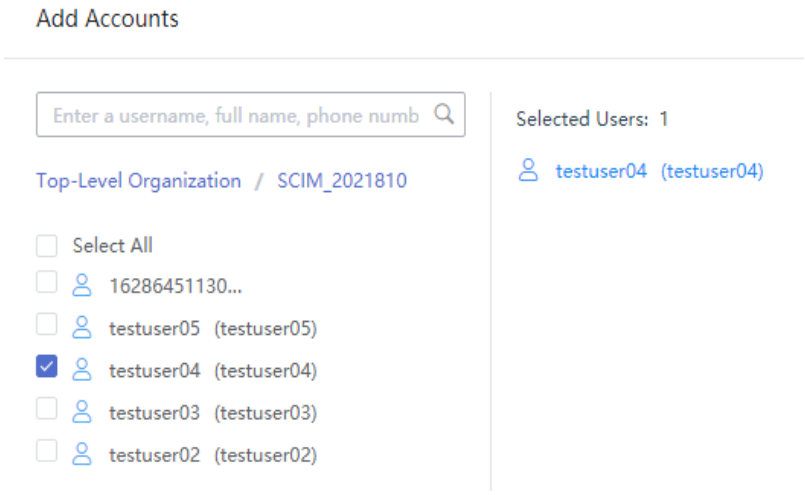
  For details about how to configure login, access control, and object models, see **Modifying Application Configurations**.

Figure 2-15 Adding accounts



 Copyright © Huawei Technologies Co., Ltd.

Figure 2-16 Selecting users



Establishing a Trust Between the Application and OneAccess

Configure authorization information for OneAccess in the application to establish a trust on OneAccess.

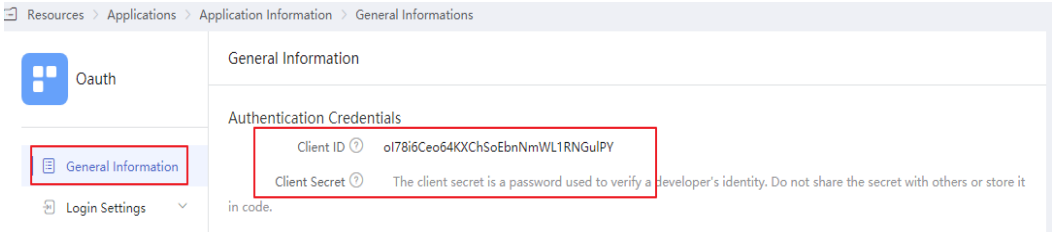
Step 1 Obtain the Client ID and ClientSecret of the application in OneAccess.

Click the application added in **Adding an Application**, click the application icon on the application information page, and obtain the Client ID and ClientSecret.

NOTE

- To obtain a ClientSecret, click **Enable** to generate one.
- ClientSecret is an important credential used to verify the identity of a developer. Do not provide the ClientSecret to other developers or store it in code.
- If you reset the ClientSecret, the new ClientSecret takes effect immediately, and all interfaces that use the old ClientSecret become invalid. Exercise caution when performing this operation.
- OneAccess does not store the ClientSecret. Keep it properly after obtaining it.

Figure 2-17 Obtaining the Client ID and ClientSecret



Step 2 Obtain the authentication information in OneAccess.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Settings** > **Server Settings**. Then click **OIDC**.
3. On the **OIDC** page, view the authentication address.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Obtain the authorization information of the application. For details, see the application provider's documentation.

----End

Logging In as a User

Log in to the user portal as one of the **authorized users**, and click the target application to check whether you can access it.

2.3 SSO Access to Applications Through OIDC

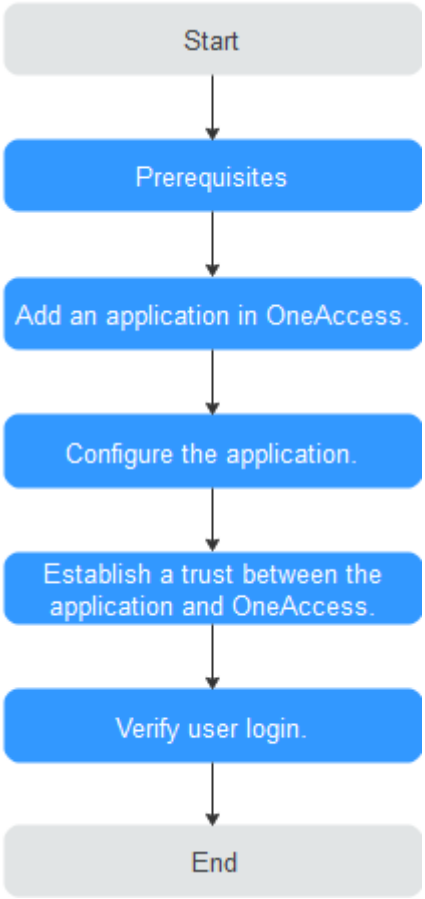
Introduction

OpenID Connect (OIDC) is an interoperable authentication protocol based on the OAuth 2.0 family of specifications. For details, see **Welcome to OpenID Connect**.

This section describes how to integrate an application with OneAccess using the OIDC protocol.

Configuration Process

Figure 2-18 Configuration process



 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

You have permissions to access the administrator portal.

Adding an Application

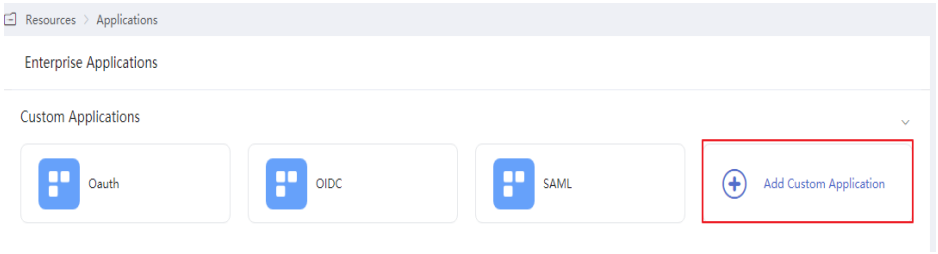
Add an application in the administrator portal, and configure authentication information to establish a trust on it.

Step 1 Log in to the administrator portal.

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

Step 3 Click **Add Custom Application** in the **Custom Applications** section, set the logo and application name, and click **Save**.

Figure 2-19 Adding a custom application



----End

Configuring the Application

Configure the application in OneAccess so that users can log in to the application through OneAccess. For details, see **authentication configuration**, **mapping configuration (optional)**, and **user authorization**.

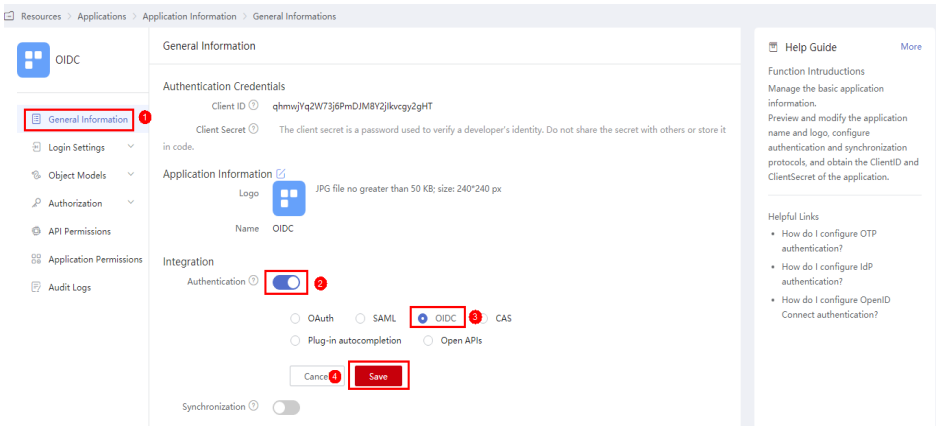
- Authentication configuration
  a. Click the application added in **Adding an Application** and click the application icon on the application information page.
  b. On the application details page, choose **General Information** > **Integration**, enable authentication, select **OIDC**, and click **Save**.

  NOTE

  The protocol cannot be changed once specified.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-20 Selecting an authentication protocol



c. Click **Authentication Settings** in the left pane, and configure the authentication parameters.

CAUTION

To avoid information leakage, do not include sensitive information in the configuration parameters.

Figure 2-21 Configuring authentication parameters

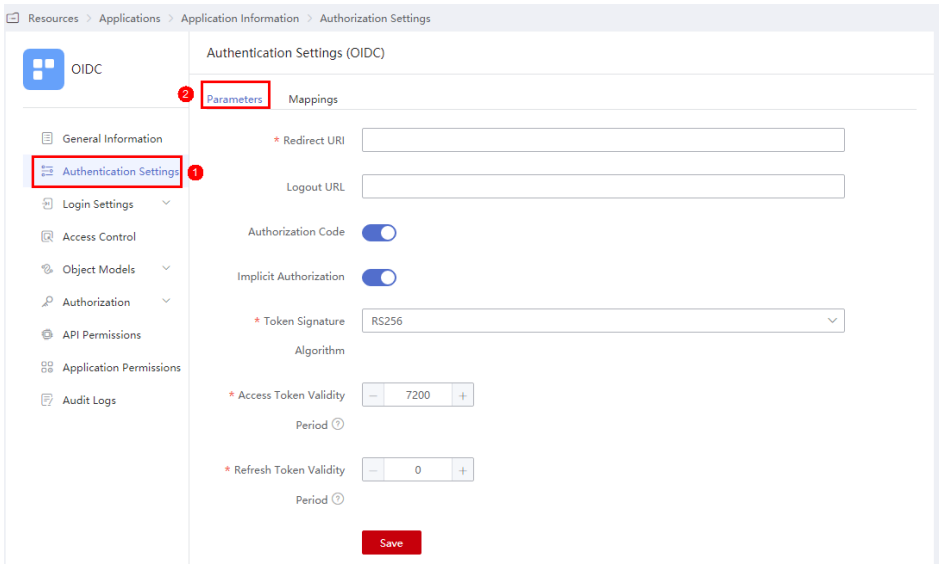


Table 2-6 Authentication parameters

Parameter	Description
Redirect URL	(Required) Callback URL to be visited after successful authorization. Enter a trusted domain name, and separate multiple domain names using commas (,) if any. The application homepage is recommended, for example, **https://xxx.xxx.com**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Logout URL	(Optional) Logout URL to be visited after a user logs out of their session.
Authorization Code	Enabled by default. This mode is the most widely used authentication mode and is suitable for applications whose frontend and backend are separated. For details about the authorization code mode, see **Introduction**.
Implicit Authentication	Enabled by default. This mode does not require an authorization code and is suitable for applications that do not have a backend.
Token Signature Algorithm	Algorithm used to sign tokens. By default, **RS256** is used.
Access Token Validity Period	Validity period of the access token in seconds. The default value is 7200 seconds, that is, 2 hours.
Refresh Token Validity Period	Validity period of the refresh token. The default value is **0**, indicating that the refresh token is not supported. When the access token of a user expires, the user can use their refresh token to obtain a new access token. **NOTE** The prerequisite for automatic token update is that the validity period of the refresh token is longer than that of the access token.

- (Optional) Mapping configuration
  a. On the **Authentication Settings** page, click the **Mappings** tab, and click **Add Mapping** to add an attribute mapping.

Figure 2-22 Adding a mapping

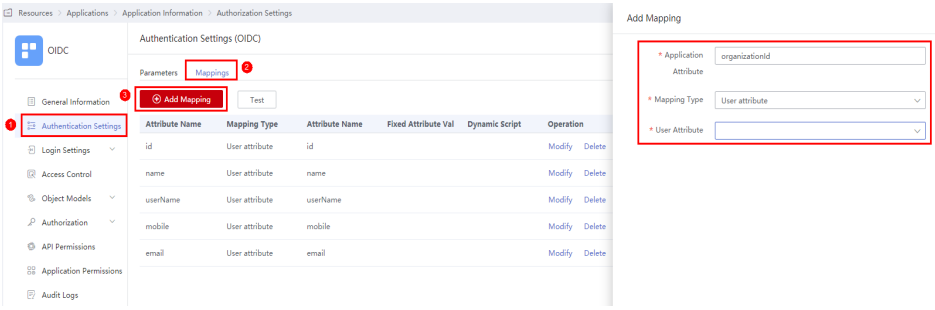


Table 2-7 Mapping parameters

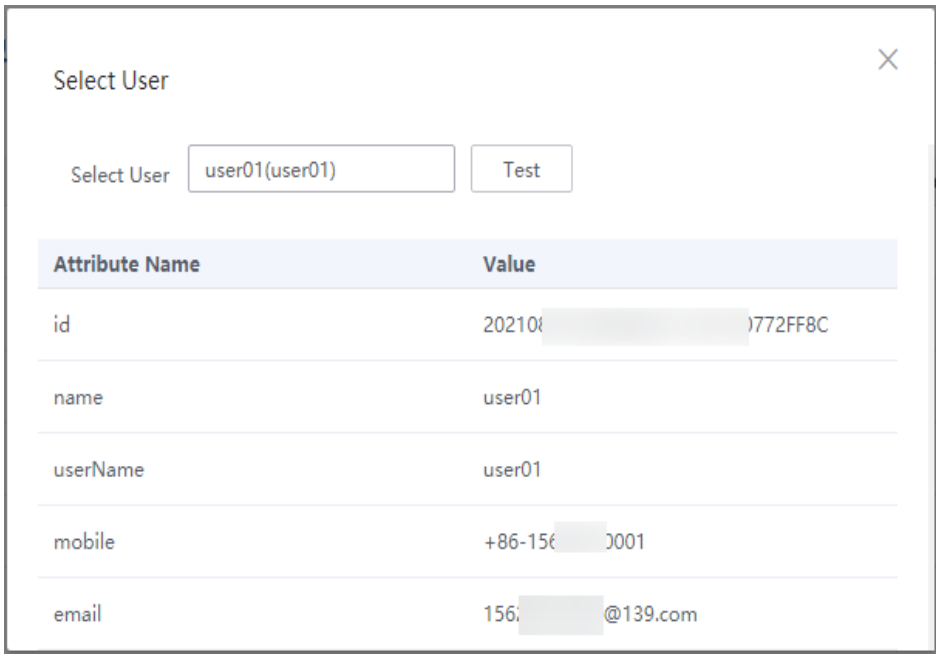
Parameter	Description
Application Attribute	(Required) User attribute that OneAccess will return to the application after successful authentication.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Mapping Type	(Required) The mapping type determines the returned attribute value.
User Attribute	(Required) Attribute mapped from OneAccess to the application.

b. Click **Test**. On the **Select User** page, enter a username to test the mappings.

Figure 2-23 Testing mappings



- User authorization

  In the left pane, choose **Authorization** > **Application Accounts**. Then click **Add Accounts** to authorize specific users to access the application. To authorize access using a policy, see the descriptions about the application account authorization policy in **Modifying Application Configurations**.

  NOTE

  For details about how to configure login, access control, and object models, see **Modifying Application Configurations**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-24 Adding accounts

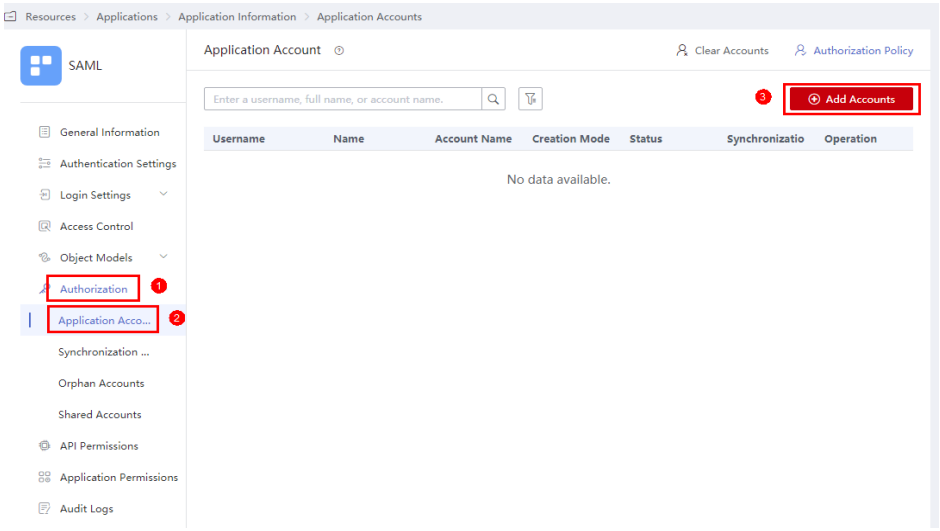
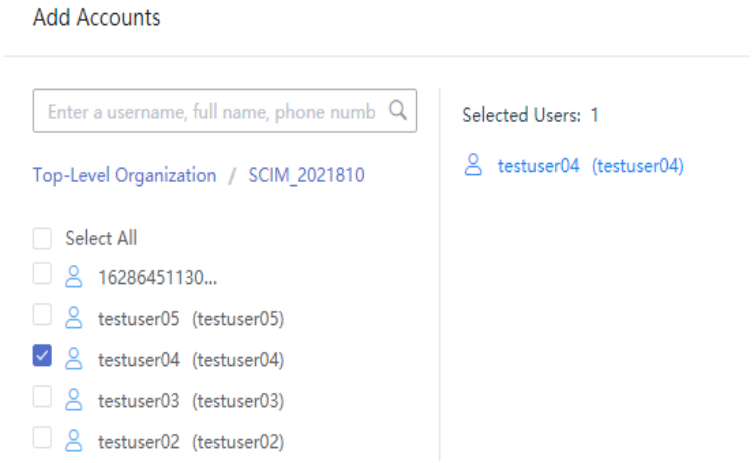


Figure 2-25 Selecting users



Establishing a Trust Between the Application and OneAccess

Configure authorization information for OneAccess in the application to establish a trust on OneAccess.

Step 1 Obtain the Client ID and ClientSecret of the application in OneAccess.

Click the application added in **Adding an Application**, click the application icon on the application information page, and obtain the Client ID and ClientSecret.

NOTE

- To obtain a ClientSecret, click **Enable** to generate one.
- ClientSecret is an important credential used to verify the identity of a developer. Do not provide the ClientSecret to other developers or store it in code.
- If you reset the ClientSecret, the new ClientSecret takes effect immediately, and all interfaces that use the old ClientSecret become invalid. Exercise caution when performing this operation.
- OneAccess does not store the ClientSecret. Keep it properly after obtaining it.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Obtain the authentication information in OneAccess.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Settings** > **Server Settings**. Then click **OIDC**.
3. On the **OIDC** page, view the authentication address.
4. Click **OIDC Discovery** in the upper right and view the authentication parameters.

Step 3 Obtain the authorization information of the application. For details, see the application provider's documentation.

----End

Logging In as a User

Log in to the user portal as one of the **authorized users**, and click the target application to check whether you can access it.

2.4 SSO Access to Applications Through CAS

Introduction

Central Authentication Service (CAS) is an HTTP2- and HTTP3-based protocol which requires that each component can be accessed through a specific URL. You can configure OneAccess as an identity service provider through CAS to enable third-party applications to read user account data from OneAccess. CAS 1.0, CAS 2.0, and CAS 3.0 are supported.

Learn about the **CAS protocol** and **authorization process**.

- CAS protocol

  The CAS protocol involves two entities: CAS client and CAS server. They exchange information through users' browsers. For example, a CAS client returns a redirect message containing parameters and forwards the message to the CAS server. If the login authentication is successful, the CAS server returns an XML response containing the user information to the CAS client. After authenticating the user information, the CAS client returns the requested resource to the user.

  – CAS server: identity authentication provider. For example, OneAccess can be considered as an identity authentication provider.

  – CAS client: resource provider, for example, third-party applications.

- Authorization process

  a. A user logs in to a CAS client.

  b. The CAS client checks whether the HTTP request contains a service ticket (ST). If it does not contain an ST, the user has not been authenticated. In this case, the CAS client forwards the request together with the Service (the target resource address) to the CAS server.

  c. The user enters authentication information. If the login is successful, the CAS server randomly generates a unique ST that cannot be forged, and then sends the ST to the CAS client.

 Copyright © Huawei Technologies Co., Ltd.

d. After receiving the Service and ST, the CAS client interacts with the CAS server in the background.

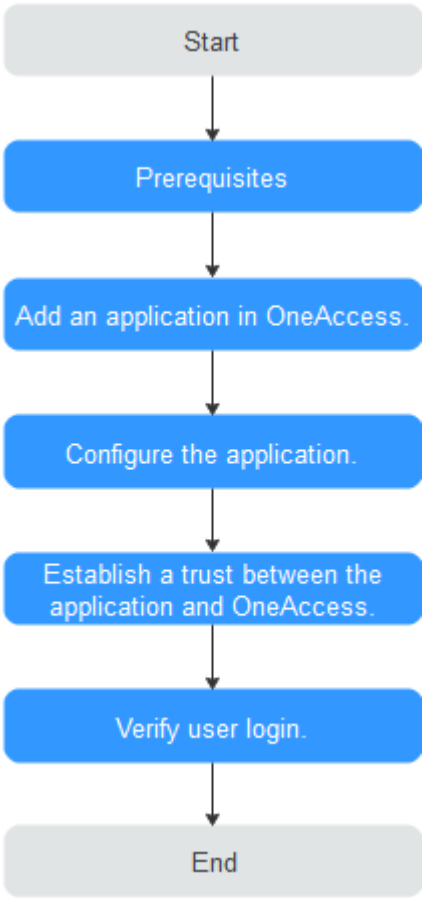
e. The CAS server verifies the user identity based on the Service and ST, and returns an XML response (containing the user information) in a specified format to the CAS client.

f. The CAS client and CAS server finish authenticating the identity of the user. The CAS client returns the requested resource to the user.

This section describes how to integrate an application with OneAccess using the CAS protocol.

Configuration Process

Figure 2-26 Configuration process



Prerequisites

You have permissions to access the administrator portal.

Adding an Application

Add an application in the administrator portal, and configure authentication information to establish a trust on it.

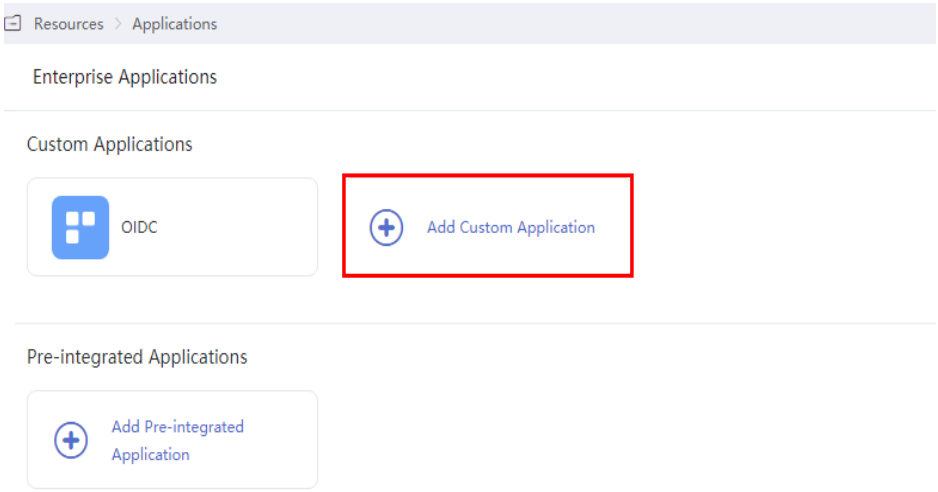
Step 1 Log in to the administrator portal.

 Copyright © Huawei Technologies Co., Ltd.

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

Step 3 Click **Add Custom Application** in the **Custom Applications** section, set the logo and application name, and click **Save**.

Figure 2-27 Adding a custom application



----End

Configuring the Application

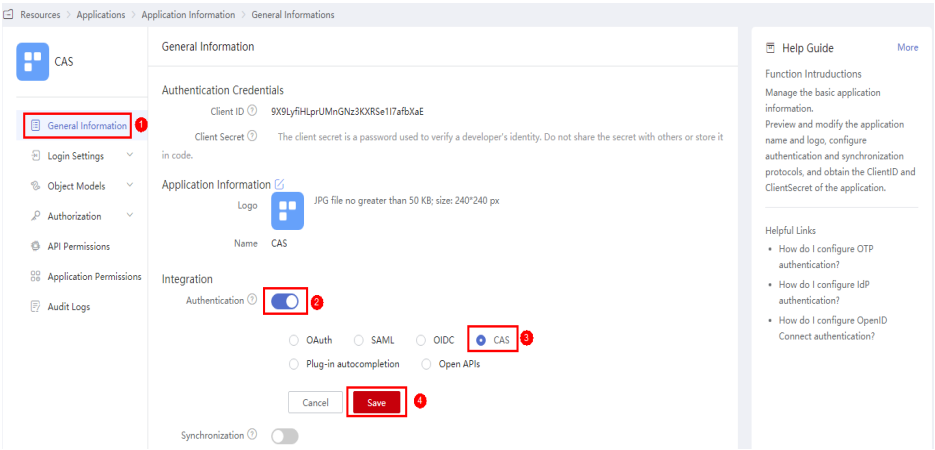
Configure the application in OneAccess so that users can log in to it through OneAccess. For details, see **authentication configuration**, **mapping configuration**, and **user authorization**.

- Authentication configuration
  a. Click the application added in **Adding an Application** and click the application icon on the application information page.
  b. On the application details page, choose **General Information** > **Integration**, enable authentication, select **CAS**, and click **Save**.

  NOTE

  The protocol cannot be changed once specified.

Figure 2-28 Selecting an authentication protocol



 Copyright © Huawei Technologies Co., Ltd.

c. Click **Authentication Settings** in the left pane, and configure the authentication parameters.

> **CAUTION**
>
> To avoid information leakage, do not include sensitive information in the configuration parameters.

Figure 2-29 Configuring authentication parameters

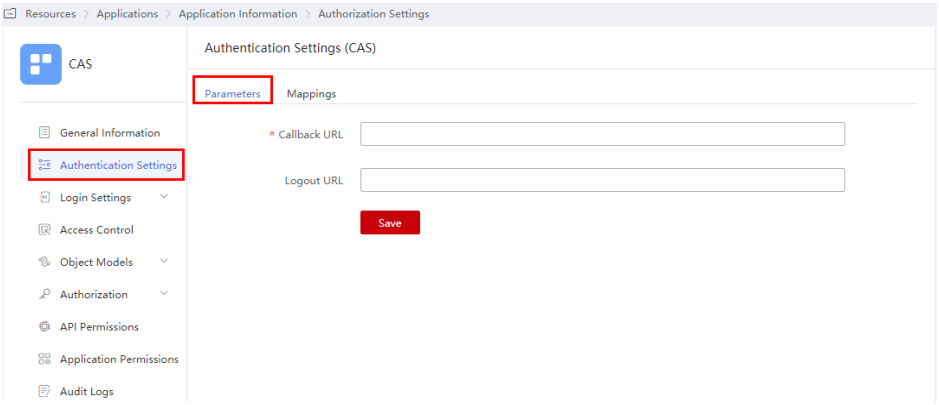


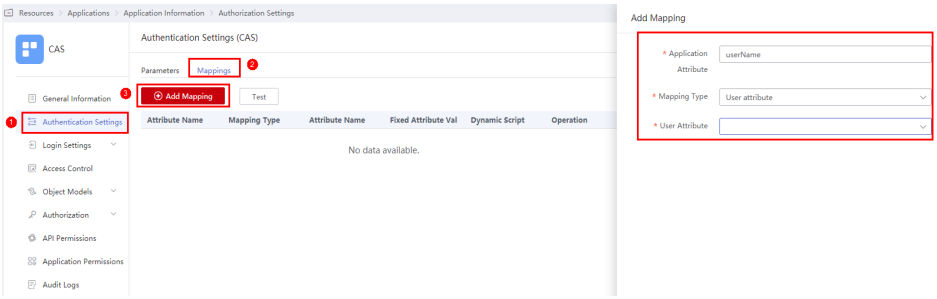
Table 2-8 Authentication parameters

Parameter	Description
Callback URL	(Required) Third-party application URL, which must be the same as the value of **service** for the CAS interface and meet the URL format requirements of RFC.
Logout URL	(Optional) Logout URL to be visited after a user logs out of their session.

- Mappings

  a. On the **Authentication Settings** page, click the **Mappings** tab, and click **Add Mapping** to add an attribute mapping.

Figure 2-30 Adding a mapping



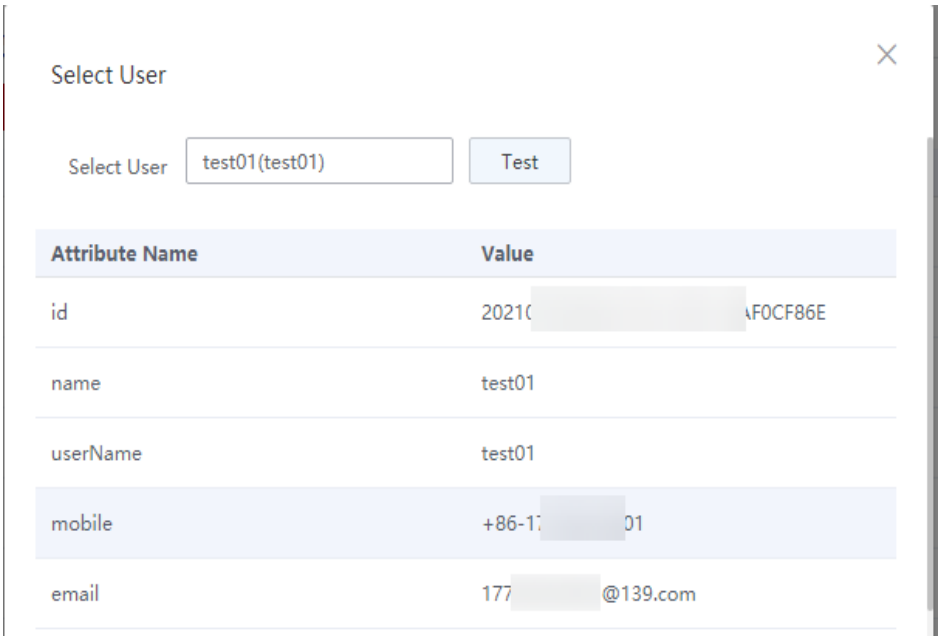
 Copyright © Huawei Technologies Co., Ltd.

Table 2-9 Mapping parameters

Parameter	Description
Application Attribute	(Required) User attribute that OneAccess will return to the application after successful authentication.
Mapping Type	(Required) The mapping type determines the returned attribute value.
User Attribute	(Required) Attribute mapped from OneAccess to the application.

b. Click **Test**. On the **Select User** page, enter a username to test the mappings.

Figure 2-31 Testing mappings



- User authorization

  In the left pane, choose **Authorization** > **Application Accounts**. Then click **Add Accounts** to authorize specific users to access the application. To authorize access using a policy, see the descriptions about the application account authorization policy in **Modifying Application Configurations**.

  NOTE

  For details about how to configure login, access control, and object models, see **Modifying Application Configurations**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-32 Adding accounts

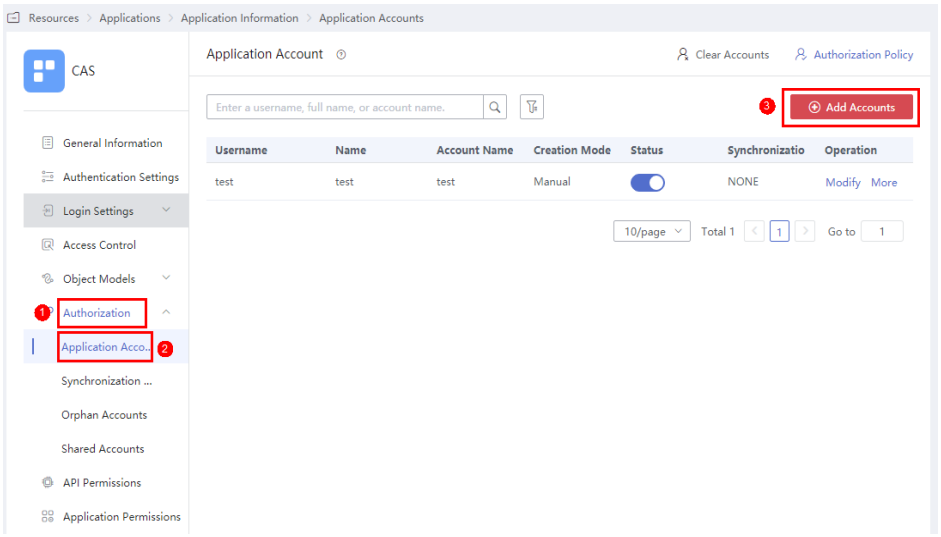
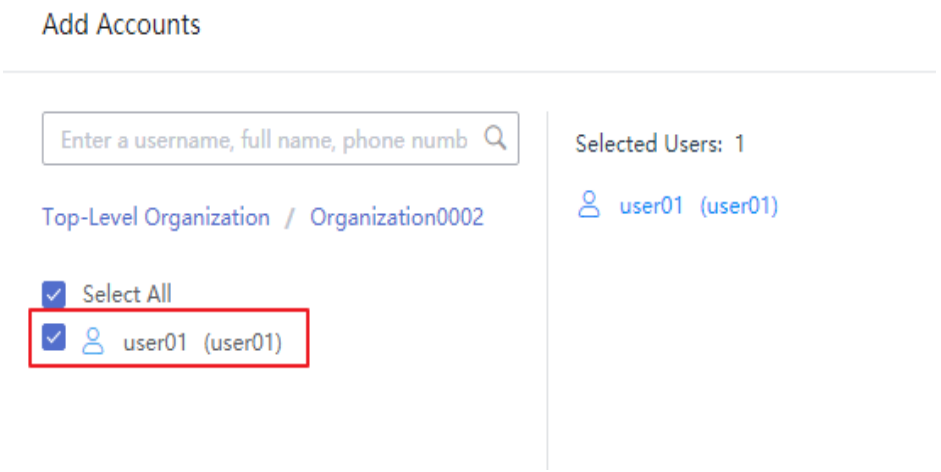


Figure 2-33 Selecting users



Establishing a Trust Between the Application and OneAccess

Configure authorization information for OneAccess in the application to establish a trust on OneAccess.

Step 1 Obtain the authentication information in OneAccess.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Settings** > **Server Settings**. Then click **CAS**.
3. On the **CAS** page, view the authentication address.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-34 Viewing CAS configurations

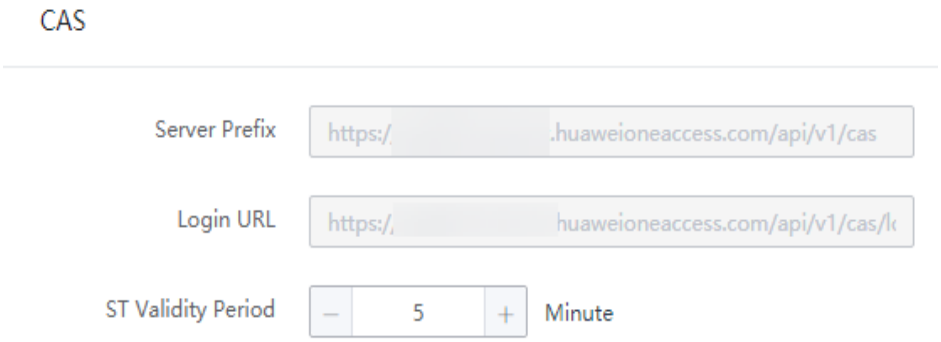


Table 2-10 Configuration parameters

Parameter	Description
Server Prefix	Prefix of the CAS server URL. The prefix is automatically generated and cannot be changed.
Login URL	Request authorization URL of the CAS server. The URL is automatically generated and cannot be changed.
ST Validity Period	Validity period of a returned ST. Set a validity period from 3 to 15 minutes.

Step 2 Obtain the authorization information of the application. For details, see the application provider's documentation.

----End

Logging In as a User

Log in to the user portal as one of the **authorized users**, and click the target application to check whether you can access it.

 Copyright © Huawei Technologies Co., Ltd.

3 Data Synchronization

Synchronizing Data to Atlassian Through SCIM

Synchronizing Data Through LDAP

3.1 Synchronizing Data to Atlassian Through SCIM

Introduction

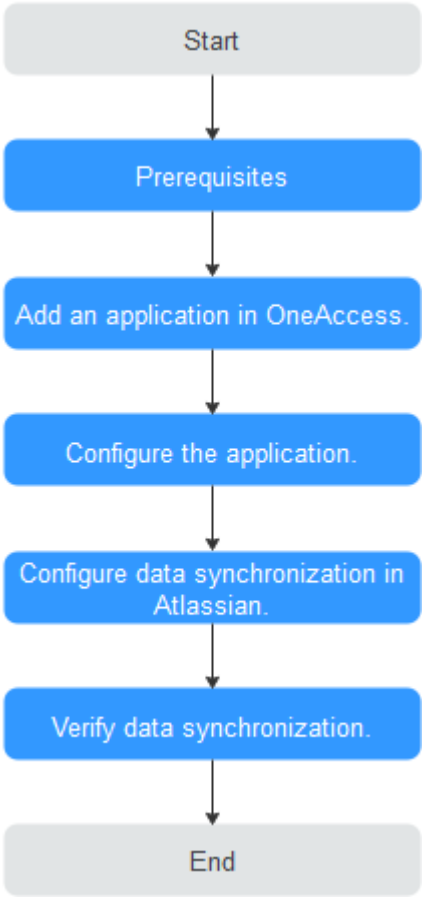
System for Cross-domain Identity Management (SCIM) is designed to manage multi-tenant identities for cloud-based applications. SCIM 2.0 is built on an object model where a resource is the common denominator and all SCIM objects are derived from it. SCIM 2.0 has **id**, **externalId**, and **meta** as attributes. RFC 7643 defines **User**, **Group**, and **EnterpriseUser** that extend the common attributes. For details about SCIM, see **SCIM Overview**.

This section describes how to synchronize user data to Atlassian through the SCIM protocol.

Configuration Process

Configuration process

 Copyright © Huawei Technologies Co., Ltd.



Prerequisites

- You have an administrator account for Atlassian.
- You have permissions to access the administrator portal.

Adding an Application

Step 1 Log in to the administrator portal.

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

Step 3 Click **Add Custom Application** in the **Custom Applications** section, set the logo and application name, and click **Save**.

----End

Configuring the Application

Step 1 Click the application added in **Adding an Application** and click the application icon on the application information page.

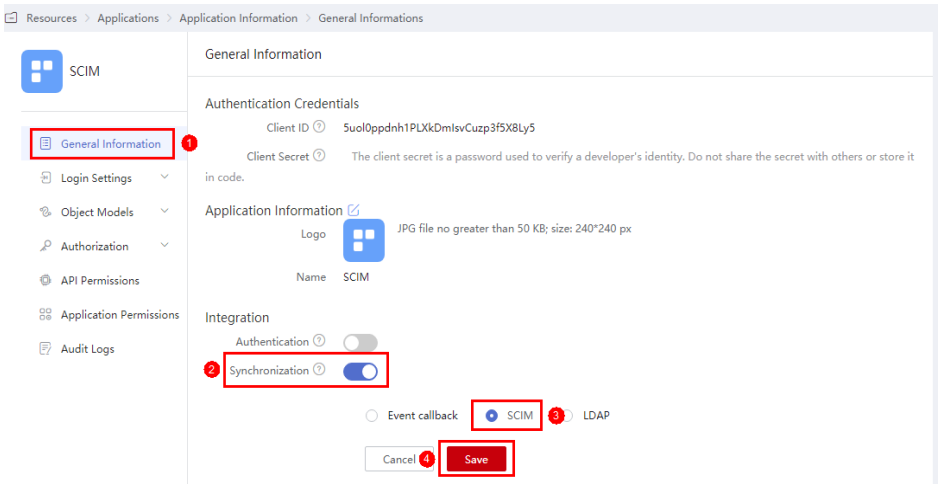
Step 2 On the application details page, choose **General Information** > **Integration**, enable synchronization, select **SCIM**, and click **Save**.

NOTE

The protocol cannot be changed once specified.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-1 Selecting a synchronization protocol



Step 3 Click **Synchronization Settings** in the left pane, and configure the synchronization parameters.

Figure 3-2 Configuring synchronization parameters

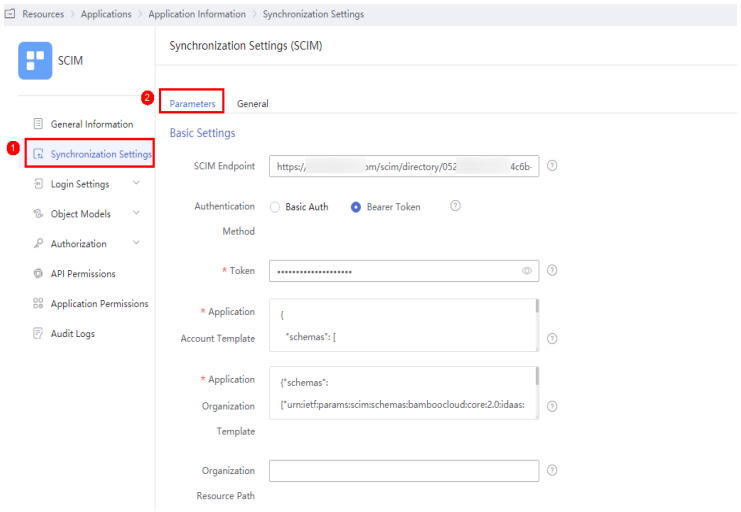


Table 3-1 Basic settings

Parameter	Mandatory	Description
SCIM Endpoint	Yes	Interface address of the target system to receive SCIM data, for example, **https://example.com/v2**.
Authentication Method	Yes	The default authentication method is **Basic Auth**.
Username	Yes	Username for authentication. Set this parameter if you specify the authentication method as **Basic Auth**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
Password	Yes	Password of the user. Set this parameter if you specify the authentication method as **Basic Auth**.
Token	Yes	Authorization token, which you can obtain from the application.
Application Account Template	Yes	Template of user request data to be pushed to the target system. By default, the data template of SCIM 2.0 is used. Set the template according to the SCIM version supported by the target system.
Application Organization Template	Yes	Template of organization request data to be pushed to the target system. By default, the data template of SCIM 2.0 is used. Set the template according to the SCIM version supported by the target system.
Organization Resource Path	No	Organization resource path in SCIM. For example, the user path is **User** and the user group path is **Group**.

Table 3-2 Advanced settings

Parameter	Mandatory	Description
Content-Type	No	Request header, 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	No	Request header, which you can set based on the target system. Set this parameter to **application/json** or **application/scim+json**.
Time Format	No	JSON time format. If the time is in milliseconds, set this parameter to "timestamp". If the time is another type of value, set this parameter to a format expression, for example, **yyyy-MM-dd HH:mm:ss**.

Step 4 Choose **Object Models** > **Application Account Model** in the left pane, click the **Attributes** tab, and click **Add** to add an email attribute.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-3 Adding an attribute

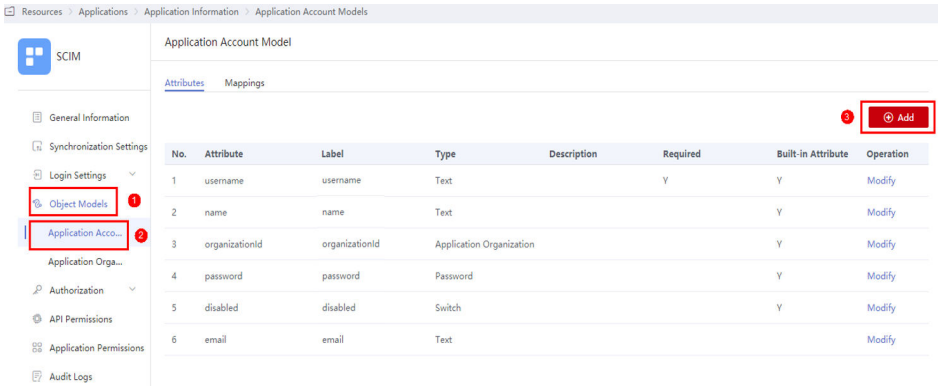


Table 3-3 Attributes

Parameter	Mandatory	Description
Attribute	Yes	Attribute that OneAccess will map to the target application, for example, **email**.
Label	No	Display name of the attribute, for example, **Email Address**.
Description	No	Description about the attribute.
Attribute Type	Yes	Type of the attribute, for example, **Text**.
Required field	No	Indicates whether the attribute is required.

Step 5 Switch to the **Mappings** tab page, click **Modify**, and configure the email address mapping.

Table 3-4 Mappings

Parameter	Description
User	Attribute that OneAccess will map to the application, for example, **email**.
Conversion Mode	Attribute mapping mode.
Script Expression	Enter a script if you specify the conversion mode as **Script-based**.
Execution Mode	Operation to be performed when user data is synchronized from OneAccess to the target application.

 Copyright © Huawei Technologies Co., Ltd.

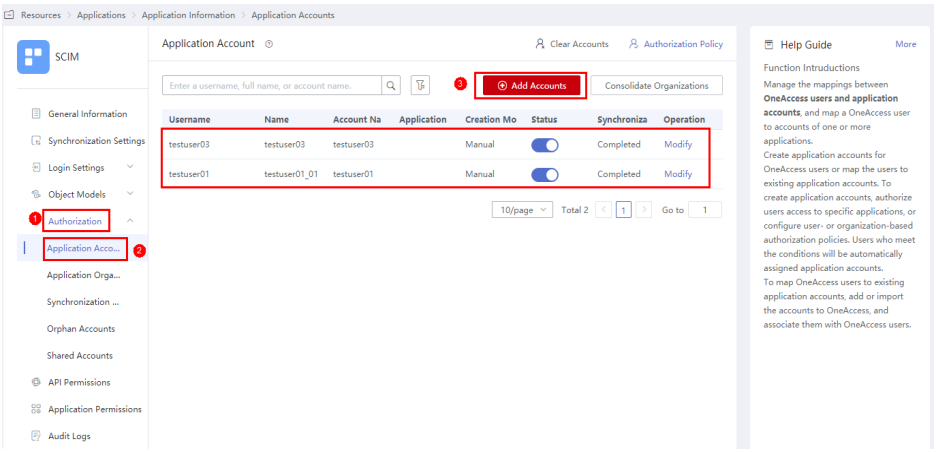
Parameter	Description
Application Account	Account attribute of the application.

Step 6 In the left pane, choose **Authorization** > **Application Accounts**. Then click **Add Accounts** to authorize specific users to access the application. To authorize access using a policy, see the descriptions about the application account authorization policy in **Modifying Application Configurations**.

NOTE

For details about how to configure object models, API permissions, and application permissions, see **Modifying Application Configurations**.

Figure 3-4 Adding accounts



----End

Configuring Synchronization in Atlassian

Step 1 Log in to **Atlassian**.

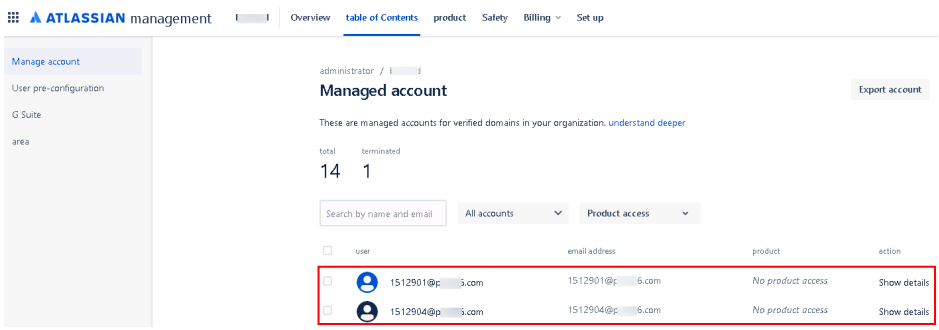
Step 2 Configure and verify the email address and set an API token. For details, see the Atlassian documentation.

----End

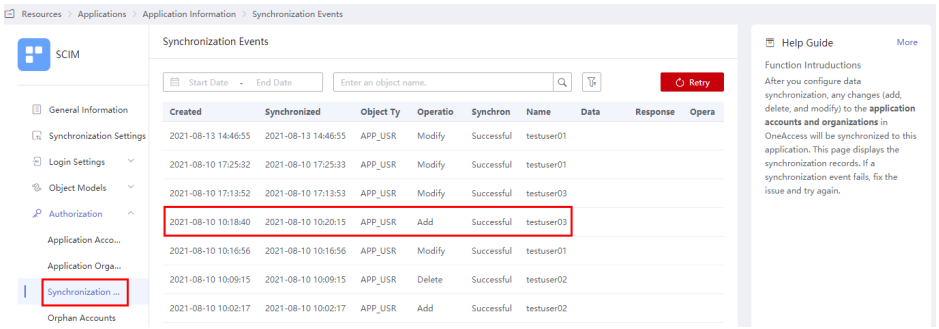
Verifying Data Synchronization

Step 1 View the synchronized users in Atlassian.

 Copyright © Huawei Technologies Co., Ltd.



Step 2 View the synchronization events in OneAccess.



----End

3.2 Synchronizing Data Through LDAP

LDAP is short for Lightweight Directory Access Protocol.

- LDAP can be considered a tree-like database that stores user and organization information.
- One of the main application scenarios of LDAP is SSO where users are automatically logged in to intranet of their company after logging in on a PC for once.

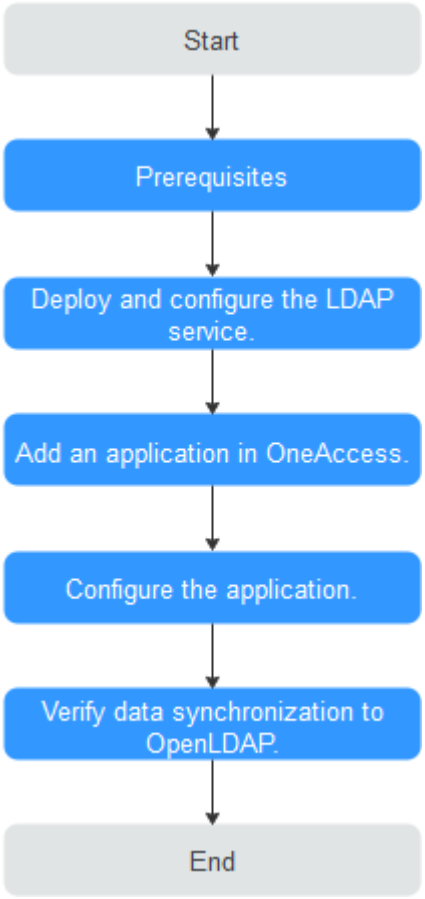
Table 3-5 Terms

Term	Description
ou	Organization unit (ou), which is a container object.
dc	Domain component (dc) is a part of a domain name.
sn	Short for surname.
cn	Short for common name.
dn	Short for distinguished name (dn). Each dn must be unique.
uid	Short for user ID.
rdn	Relative distinguished name (RDN) is similar to the relative path in the file system.

 Copyright © Huawei Technologies Co., Ltd.

This section describes how to synchronize organization and user data to OpenLDAP through the LDAP protocol.

Configuration process



Prerequisites

You have permissions to access the administrator portal.

Deploying and Configuring the LDAP Service

Deploy and configure the LDAP service. For details, see **Setting Up an LDAP Server** and **Configuring LDAP Connection**.

Adding an Application

Step 1 Log in to the administrator portal.

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

Step 3 Click **Add Custom Application** in the **Custom Applications** section, set the logo and application name, and click **Save**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Configuring the Application

Step 1 Click the application added in **Adding an Application** and click the application icon on the application information page.

Step 2 On the application details page, choose **General Information** > **Integration**, enable synchronization, select **LDAP**, and click **Save**.

NOTE

The protocol cannot be changed once specified.

Step 3 Choose **Synchronization Settings** in the left pane, click the **Parameters** tab, and configure the synchronization parameters.

Figure 3-5 Configuring synchronization parameters

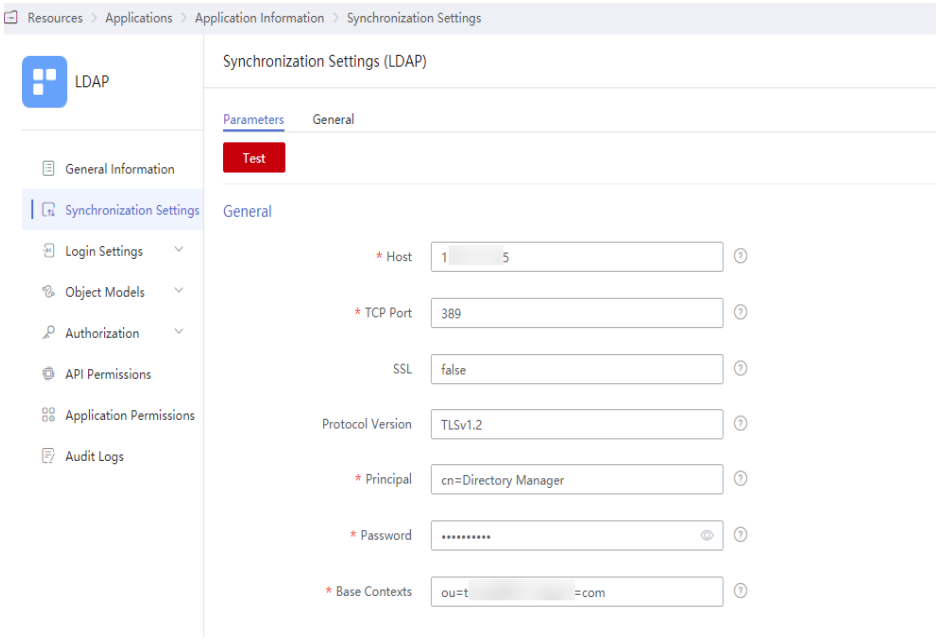


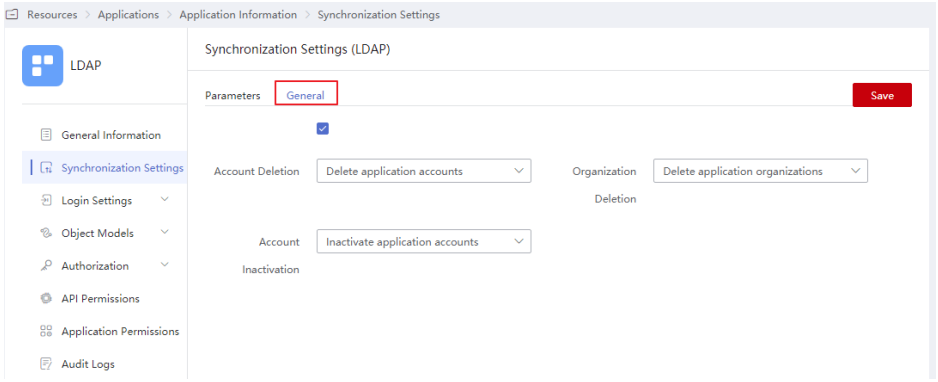
Table 3-6 Common parameters

Parameter	Description
* Host	Host name or IP address of the LDAP server.
TCP Port	TCP/IP port of the LDAP server.
SSL	Default value: **true**, which indicates that SSL is used to connect the LDAP server.
Protocol Version	Default value: **TLSv1.2**. Recommended: **TLSv1.3** and **TLSv1.2**.
Principal	Identifier used to verify the LDAP server.
Password	Authentication password of the principal.
* Base Contexts	Top-level node in the LDAP directory to be synchronized.

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Once configured, click **Save**. To test the connectivity, click **Test**.

Step 5 Go to the **General** tab page, and configure the data processing logic.



Step 6 To synchronize other user attributes, choose **Object Models** > **Application Account Model** in the left pane, click the **Attributes** tab, and click **Add** to add more attributes. **employeeNumber** is used for illustration.

NOTE

- Built-in attributes can be modified but cannot be deleted.
- Modify or delete non-built-in attributes by clicking **Modify** or **Delete** in the **Operation** column.

Figure 3-6 Adding an account attribute

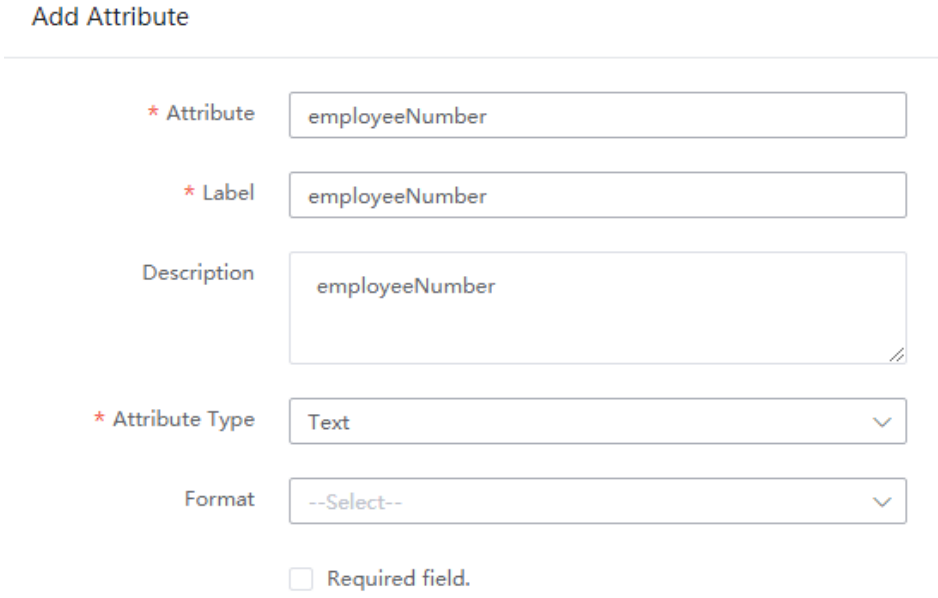


Table 3-7 Attribute definition

Parameter	Mandatory	Description
Attribute	Yes	Account attribute of the application, for example, **employeeNumber**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
Label	Yes	Customize this parameter.
Description	No	Customize this parameter.
Attribute Type	Yes	The attribute type varies depending on the attribute name and cannot be modified.
Format	No	This parameter cannot be modified.
Required field	No	Deselected by default.

Step 7 Switch to the **Mappings** tab page, click **Modify**, and configure attribute mappings.

Table 3-8 Mapping configuration

Parameter	Description
User	Attribute (such as mobile number) in OneAccess that will be mapped to the application.
Conversion Mode	Attribute mapping mode.
Script Expression	Enter a script if you specify the conversion mode as **Script-based**.
Execution Mode	Operation to be performed when user data is synchronized from OneAccess to the target application.
Application Account	Account attribute of the application.

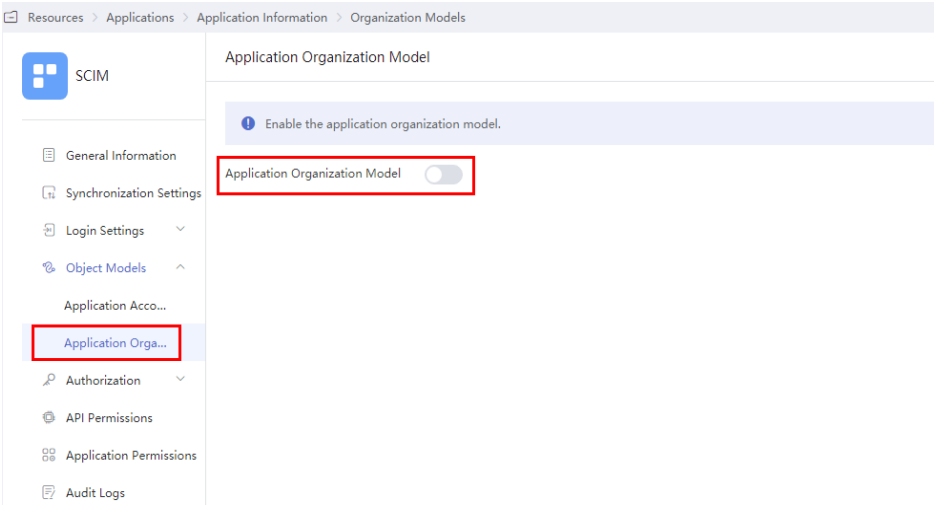
Step 8 To synchronize organizations, choose **Object Models** > **Application Organization Model**, and enable the application organization model. The model cannot be disabled once enabled.

NOTE

- Built-in attributes can be modified but cannot be deleted.
- Modify or delete non-built-in attributes by clicking **Modify** or **Delete** in the **Operation** column.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-7 Enabling the application organization model



Step 9 To synchronize other organization attributes, choose **Object Models** > **Application Organization Model** in the left pane, click the **Attributes** tab, and click **Add** to add more attributes.

Figure 3-8 Adding an organization attribute

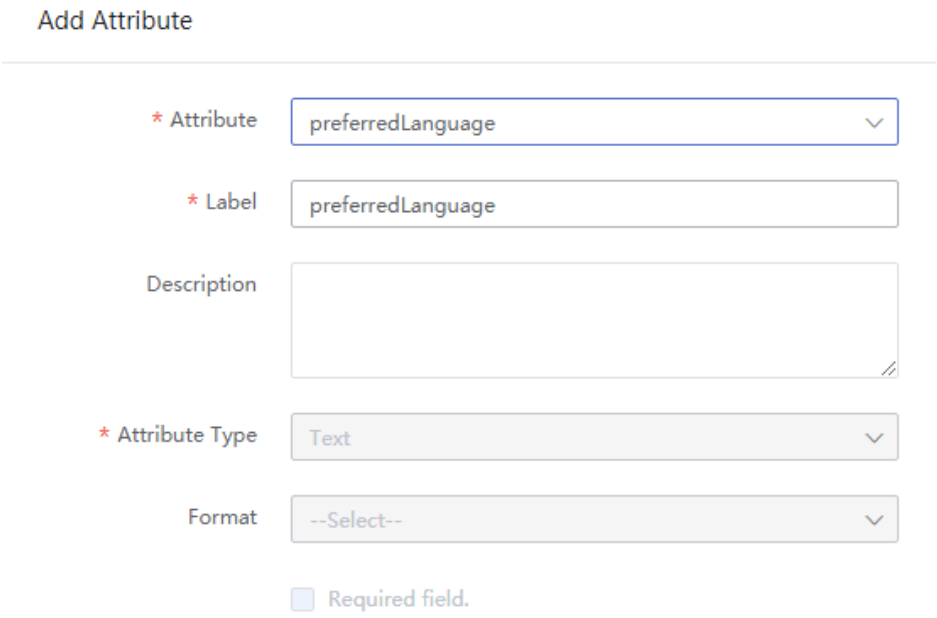


Table 3-9 Attribute definition

Parameter	Mandatory	Description
Attribute	Yes	Organization attribute of the application.
Label	Yes	Customize this parameter.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
Description	No	Customize this parameter.
Attribute Type	Yes	The attribute type varies depending on the attribute name and cannot be modified.
Format	No	This parameter cannot be modified.
Required field	No	Deselected by default. It cannot be modified.

Step 10 Switch to the **Mappings** tab page, click **Modify**, and configure attribute mappings.

Table 3-10 Mapping configuration

Parameter	Description
Organization	Organization attribute in OneAccess that will be mapped to the application.
Conversion Mode	Attribute mapping mode.
Script Expression	Enter a script if you specify the conversion mode as **Script-based**.
Execution Mode	Operation to be performed when organization data is synchronized from OneAccess to the target application.

----End

Verifying Data Synchronization to OpenLDAP

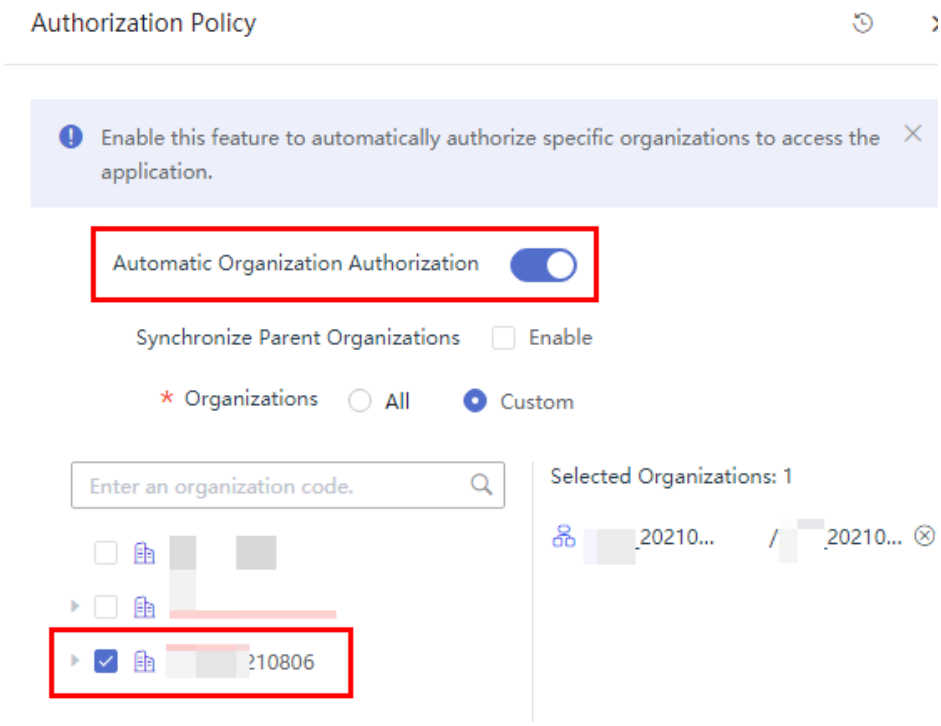
Step 1 On the application details page, choose **Authorization** > **Application Organizations** in the left pane. Click **Authorization Policy**, enable automatic organization authorization, select organizations to be synchronized, click **Save**, and then click **Add**.

NOTE

- To delete synchronized organizations, deselect the organizations, click **Save**, and then click **Delete**.
- To add a virtual organization, click **+** in the lower left.

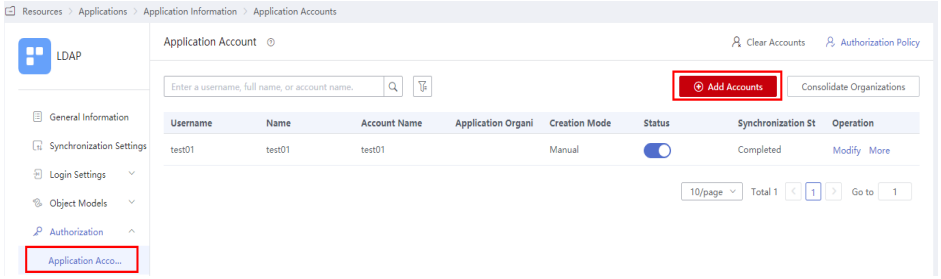
 Copyright © Huawei Technologies Co., Ltd.

Figure 3-9 Authorizing organizations



Step 2 In the left pane, choose **Authorization** > **Application Accounts**. Then click **Add Accounts** to authorize specific users to access the application. To authorize access using a policy, see the descriptions about the application account authorization policy in **Modifying Application Configurations**.

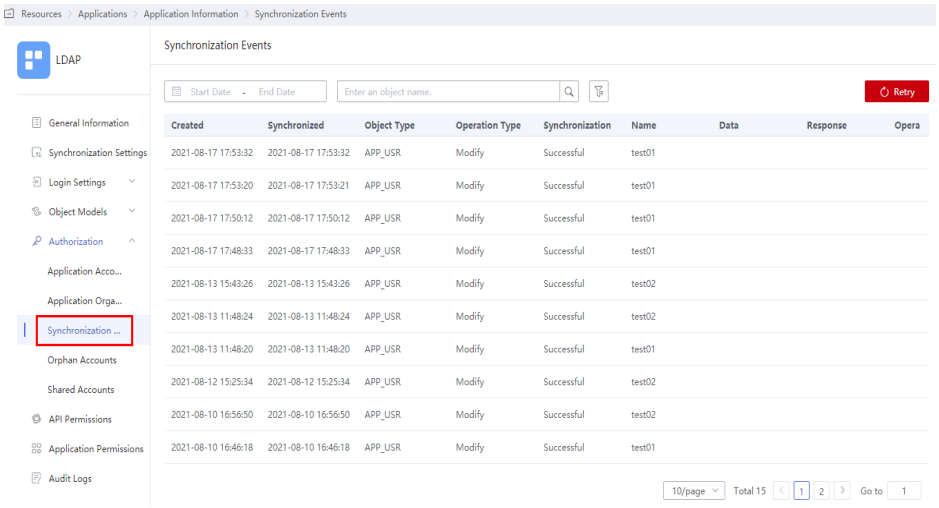
Figure 3-10 Adding accounts



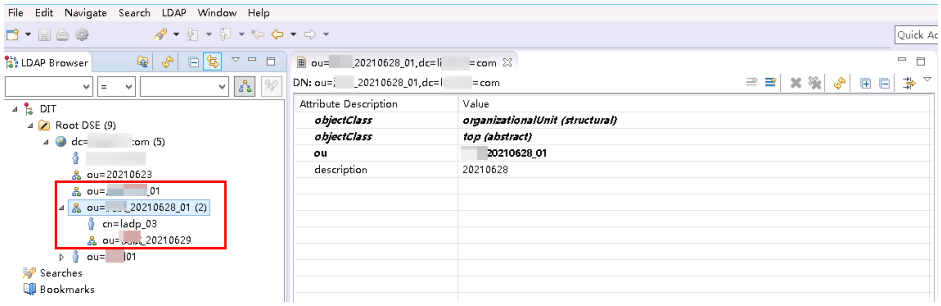
Step 3 Choose **Authorization** > **Synchronization Events** in the left pane, and view the synchronization records. You can view and filter the organization and user modification and deletion records.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-11 Viewing the synchronization events



Step 4 View the synchronized data in LDAP.



----End

 Copyright © Huawei Technologies Co., Ltd.

4 Authentication Provider Integration

SAML Authentication
OIDC Authentication
CAS Authentication
OAuth Authentication
AD Authentication
LDAP Authentication
Kerberos Authentication
eteams Authentication

4.1 SAML Authentication

Introduction

OneAccess supports SAML-based identity authentication. If you already have an identity system, configure a SAML authentication provider in OneAccess to enable users to log in to the OneAccess user portal using their IdP accounts.

Basic Concepts

- IdP

  An IdP collects and stores user identity information (such as usernames and passwords), and authenticates users when they log in. For identity authentication between your enterprise and OneAccess, IdP refers to the identity provider of your enterprise.

- SP

  An SP uses the user information provided by a trusted IdP to provide services for users. For identity authentication between your enterprise and OneAccess, SP refers to OneAccess.

- SSO

  SSO is an access type that allows users to access a trusted SP system after logging in to the enterprise IdP. For example, after a trust relationship is

 Copyright © Huawei Technologies Co., Ltd.

established between an IdP and OneAccess, users in the IdP can use their existing accounts and passwords to access OneAccess through the login link in the IdP.

- SAML 2.0

  SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about an end user between an IdP and SP. It is an open standard ratified by the Organization for the Advancement of Structured Information Standards (OASIS) and is being used by many IdPs. For more information about this standard, see **SAML 2.0 Technical Overview**. OneAccess supports SAML 2.0-based identity authentication. Enterprise IdPs used for identity authentication in OneAccess must also support SAML 2.0.

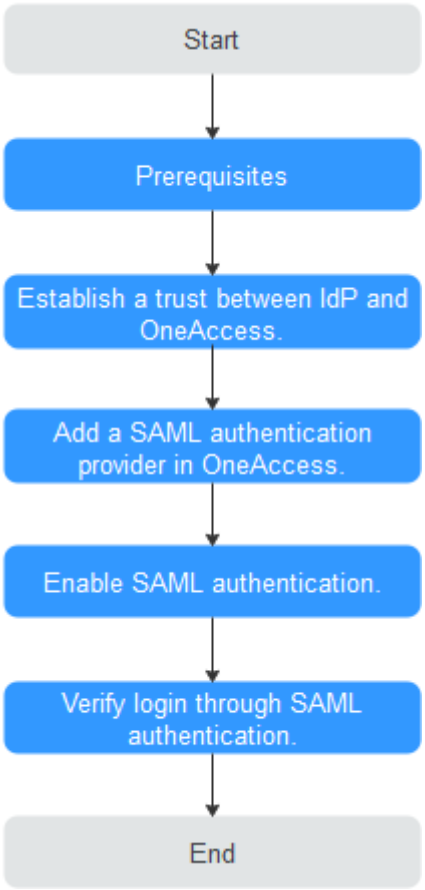
This section describes how to integrate a third-party authentication provider with OneAccess through SAML.

NOTE

The procedure for accessing the user portal on a PC is used for illustration. Configure an application that meets your service requirements.

Configuration Process

Figure 4-1 Configuration process



 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

You have permissions to access the administrator portal.

Establishing a Trust Between an IdP and OneAccess

Configure the metadata file of OneAccess in the IdP to establish a trust on OneAccess.

Step 1 Download the metadata file of OneAccess.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Authentication** > **Authentication Providers**. Then click **SAML**.
3. On the **SAML Authentication Providers** page, click **Download SP Metadata** in the upper right. The metadata is saved automatically.

Step 2 Upload the metadata file to the enterprise IdP server. For details about how to upload the metadata file, see the documentation of your enterprise IdP.

Step 3 Obtain the metadata file of the enterprise IdP. For details about how to obtain the metadata file, see the documentation of your enterprise IdP.

----End

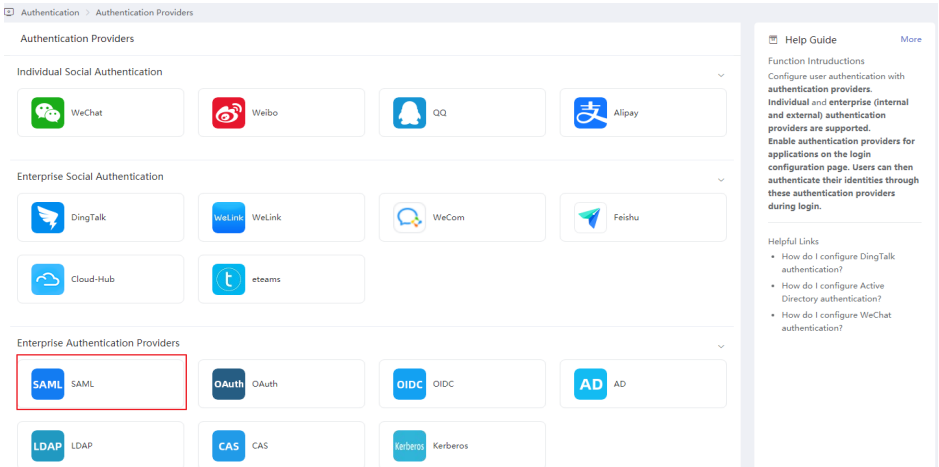
Adding a SAML Authentication Provider

Add a SAML authentication provider and configure its metadata file in OneAccess to establish a trust on the IdP.

Step 1 Log in to the administrator portal.

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

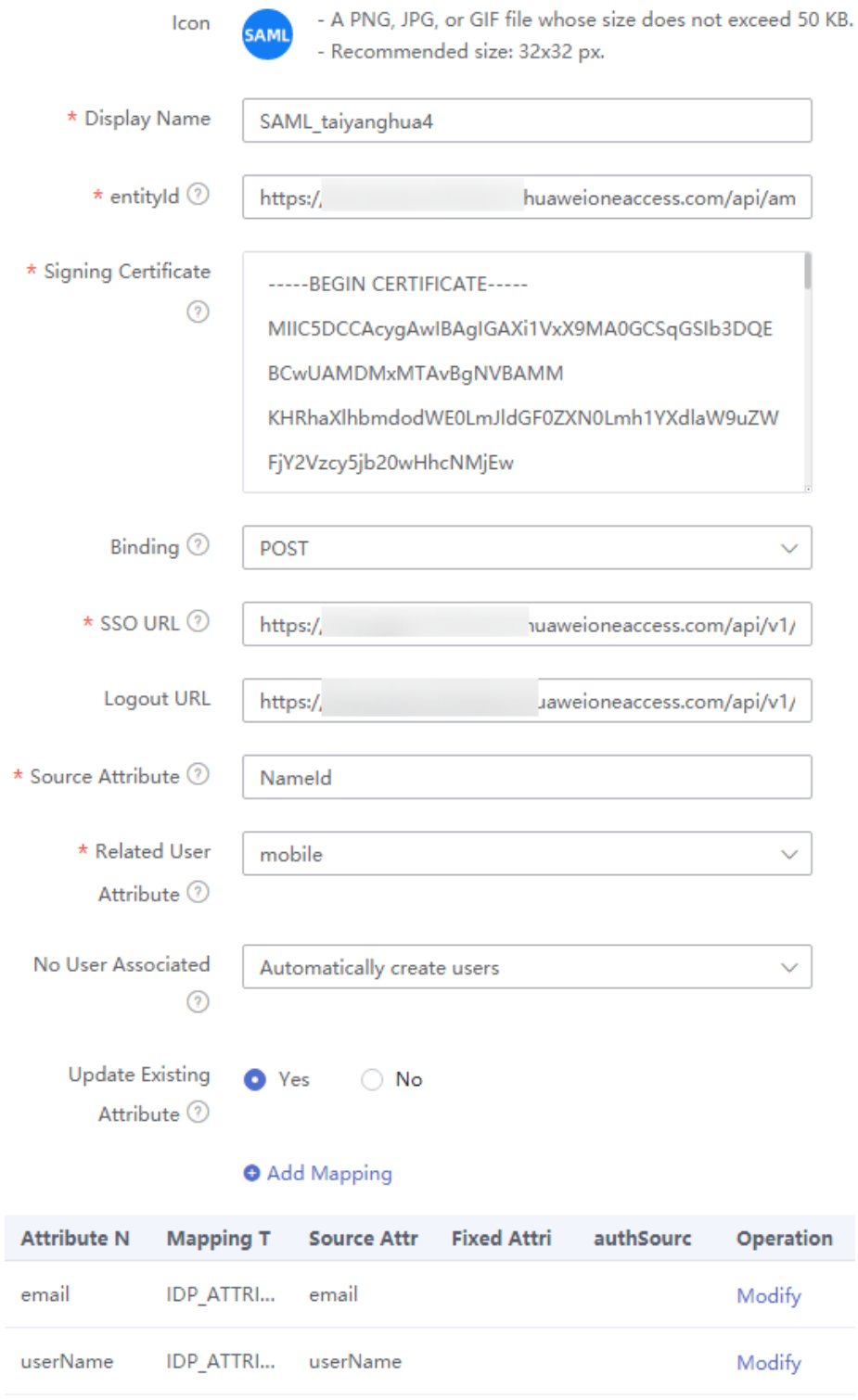
Figure 4-2 Clicking SAML



Step 3 On the **SAML Authentication Providers** page, click **Add Authentication Provider** in the upper right and set the parameters required.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-3 Configuring parameters



 Copyright © Huawei Technologies Co., Ltd.

Table 4-1 Configuration parameters

Parameter	Mandatory	Description
Icon	No	Upload a PNG, JPG, or GIF image whose size does not exceed 50 KB. The recommended size is 32 x 32 pixels.
Display Name	Yes	Display name of the authentication provider, for example, **SAML**.
entityId	Yes	Unique identifier of an identity provider. Enter the value of **entityID** contained in the IdP metadata file.
Signing Certificate	Yes	Signing certificate of the IdP, which you can obtain from the IdP's metadata file. A signing certificate is a public key certificate used for signature verification. The signing certificate is used during identity authentication to ensure that assertions are credible and complete.
Binding	Yes	Enter the value of **SingleSignOnService** displayed in the IdP's metadata file. This parameter specifies how SAML requests are sent during user login. The **SingleSignOnService** parameter in the metadata file must support HTTP Redirect or HTTP POST.
SSO URL	Yes	Enter the value of **SingleSignOnService** displayed in the IdP's metadata file.
Logout URL	No	Enter the value of **SingleLogoutService** displayed in the IdP's metadata file. This parameter indicates the URL to which users will be redirected after logging out of their sessions.
Source Attribute	Yes	Unique user attribute in the SAML assertion. This attribute must be the same as the system attribute configured in the application mappings. For example, **NameId**.
Related User Attribute	Yes	OneAccess user attribute that maps the user attribute of the SAML authentication provider. For example, **id**.
No User Associated	Yes	Operation that will be performed if a user successfully logs in through SAML authentication but fails to be associated with a system user.

To map other attributes, such as username, set **No User Associated** to **Automatically create users**, and add the desired mappings. For details, see **Table 4-2**.

 Copyright © Huawei Technologies Co., Ltd.

Table 4-2 Mapping parameters

Parameter	Description
User Attribute	Attribute (such as username) in OneAccess that maps to the SAML application.
Mapping Type	Mode of user attribute mapping between OneAccess and the SAML application.
Authentication Provider Attribute Name	User attribute in the SAML application. For details, go to the IdP platform.

----End

Enabling SAML Authentication

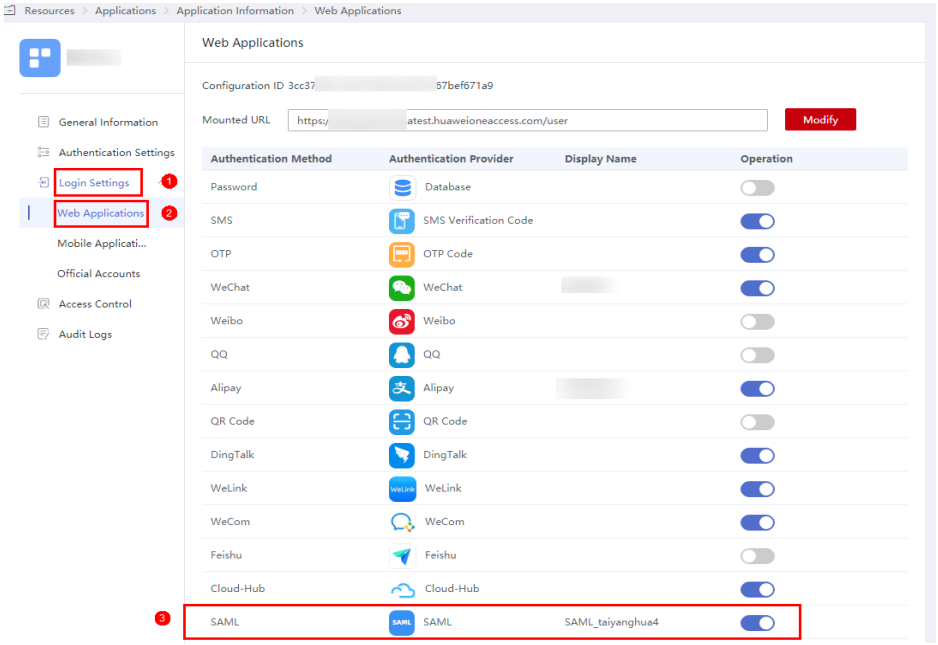
Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Resources** > **Applications**. Then select **UserCenter** in the **Pre-integrated Applications** section.

Step 3 On the application information page, click the application icon.

Step 4 On the application details page, choose **Login Settings** > **Web Applications**, enable SAML authentication, and select the authentication provider added in **Adding a SAML Authentication Provider**.

Figure 4-4 Enabling SAML authentication



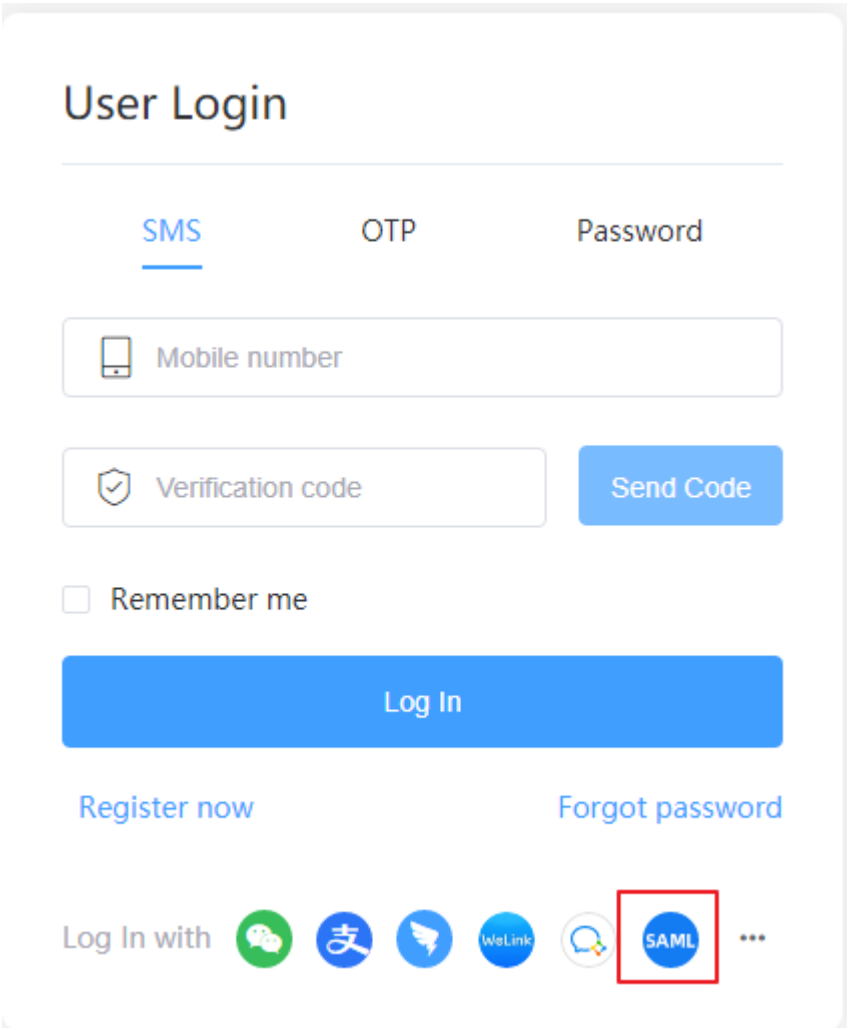
----End

 Copyright © Huawei Technologies Co., Ltd.

Logging In to the User Portal Through SAML Authentication

Step 1 Go to the user portal login page, select **SAML**, enter an IdP account and password, and click **Log In**.

Figure 4-5 Selecting SAML



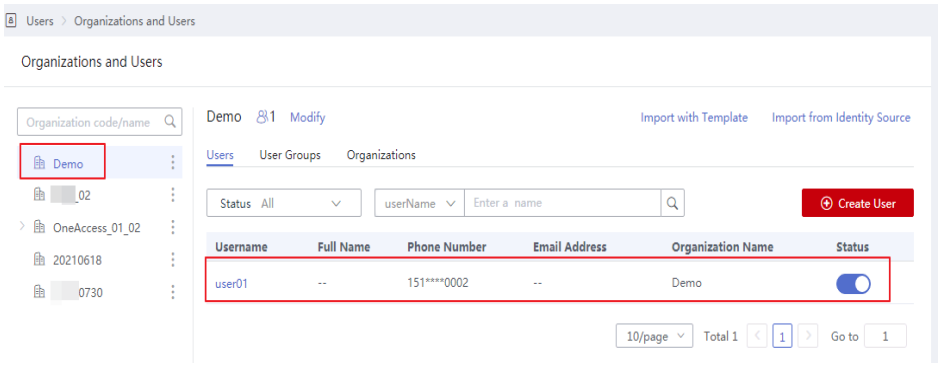
Step 2 After login, go to the administrator portal, choose **Users** > **Organizations and Users**, and view the automatically created user.

NOTE

- To automatically create a new user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 4-1**.
- By default, users automatically created in the preceding scenario belong to the first root organization on the SP side.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-6 Viewing users



----End

4.2 OIDC Authentication

Introduction

OIDC is an interoperable authentication protocol based on the OAuth 2.0 family of specifications. For details, see **Welcome to OpenID Connect**.

This section describes how to integrate a third-party authentication provider with OneAccess through OIDC. OKta is used as an example.

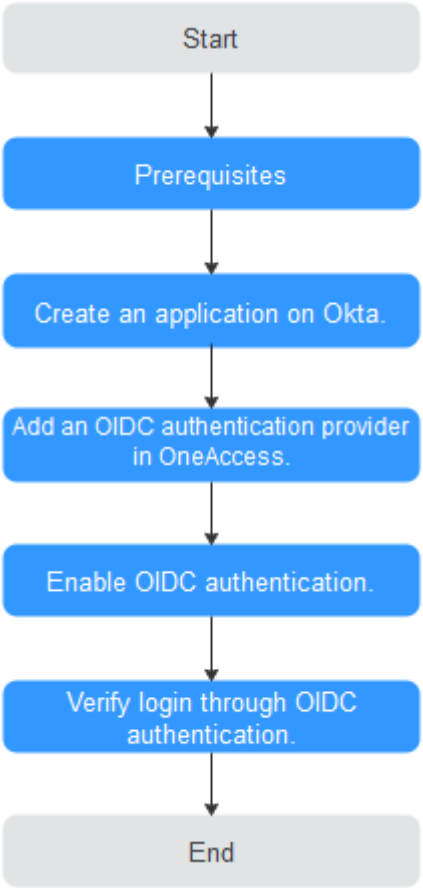
NOTE

The procedure for accessing the user portal on a PC is used for illustration. Select and configure an application that meets your service requirements.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process

Figure 4-7 Configuration process



Prerequisites

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

Creating an Application on Okta

Create an application and configure authorization information for OneAccess on the Okta platform to establish a trust on OneAccess.

Step 1 Log in to the Okta platform.

Step 2 On the Okta platform, choose **Applications** > **Add Application**, click **Create New App**, and set the application parameters. For details, see the documentation of the Okta platform.

NOTE

When you configure the application, set **Login redirect URIs** to the invocation address automatically generated for the authentication provider that you have added in OneAccess. For details, see **Table 4-3**. For example: **https://xxx.huaweioneaccess.com/api/v1/oidc/sso/2***71-8***-D***1**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-8 Configuring parameters

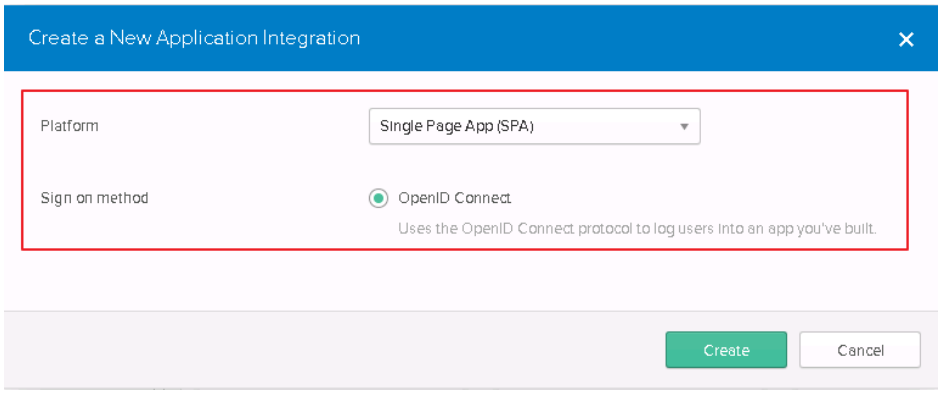
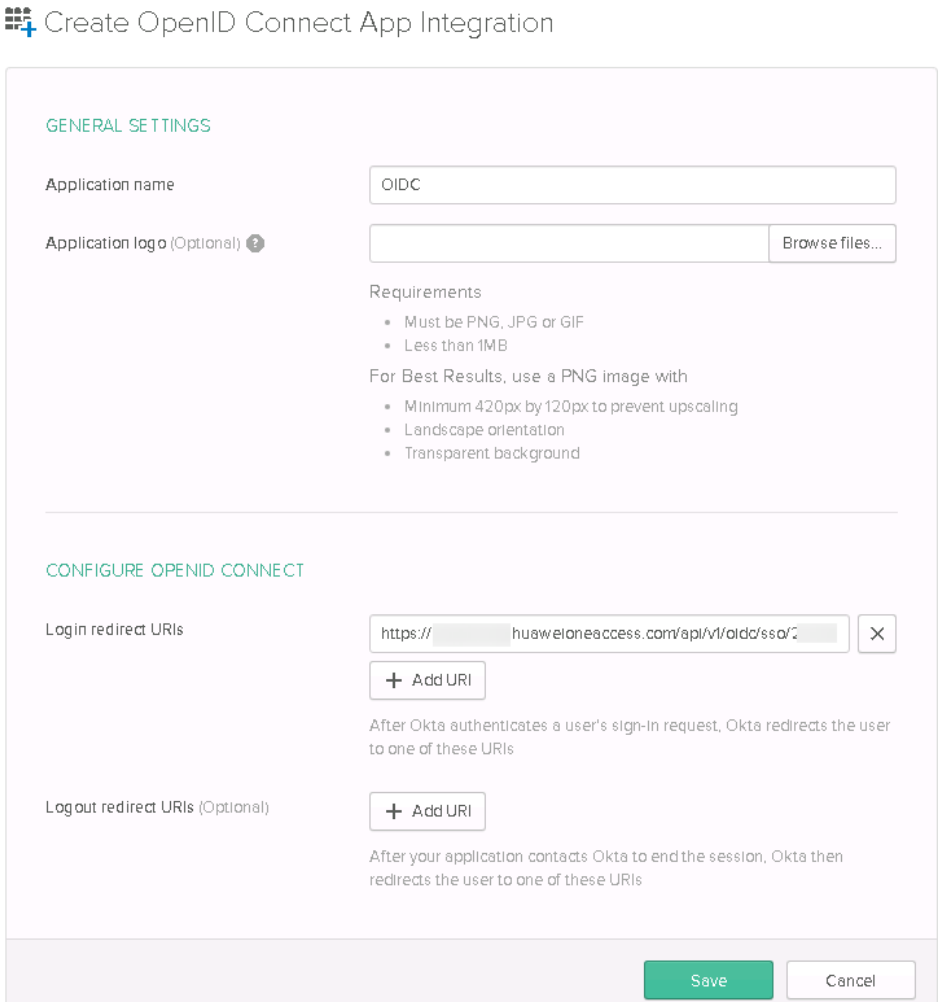


Figure 4-9 Configuring login redirect URIs



Step 3 Configure the application parameters and authorize access to specific users. For details, see the documentation of the Okta platform.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-10 Configuring application parameters

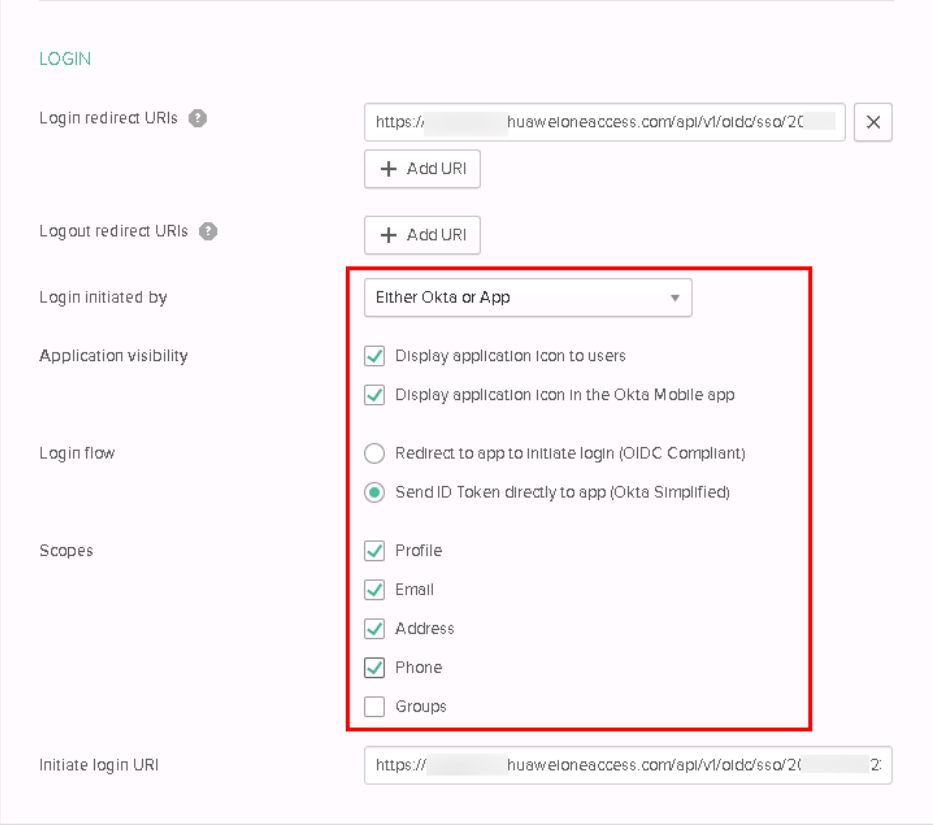
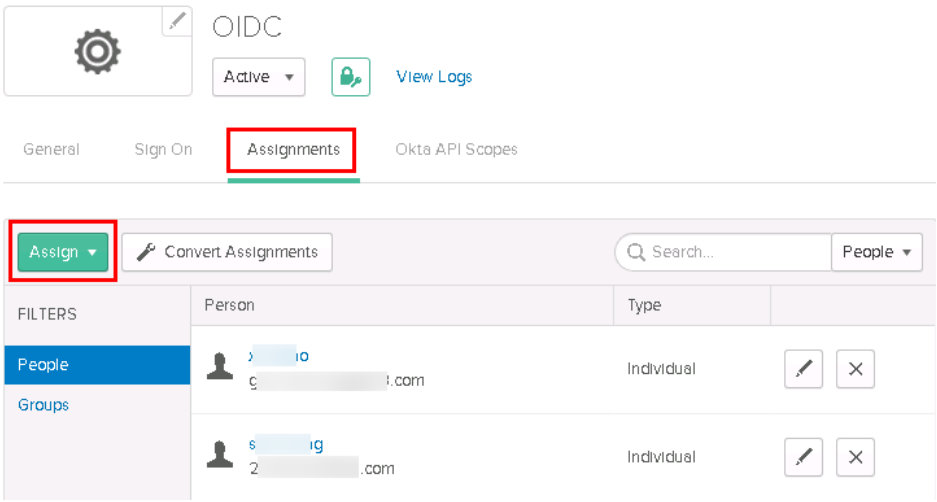


Figure 4-11 Authorizing users



----End

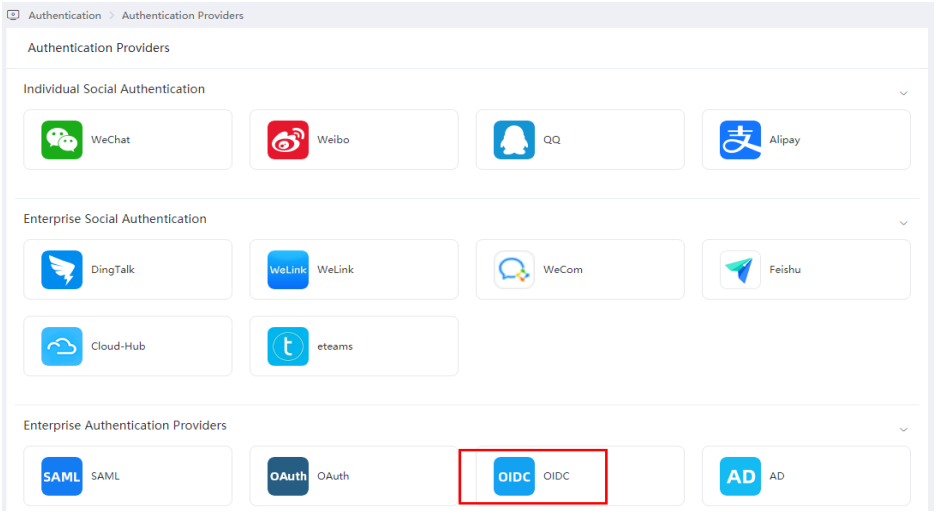
Adding an OIDC Authentication Provider

Add an OIDC authentication provider and configure the application information in OneAccess.

Step 1 Log in to the administrator portal.

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

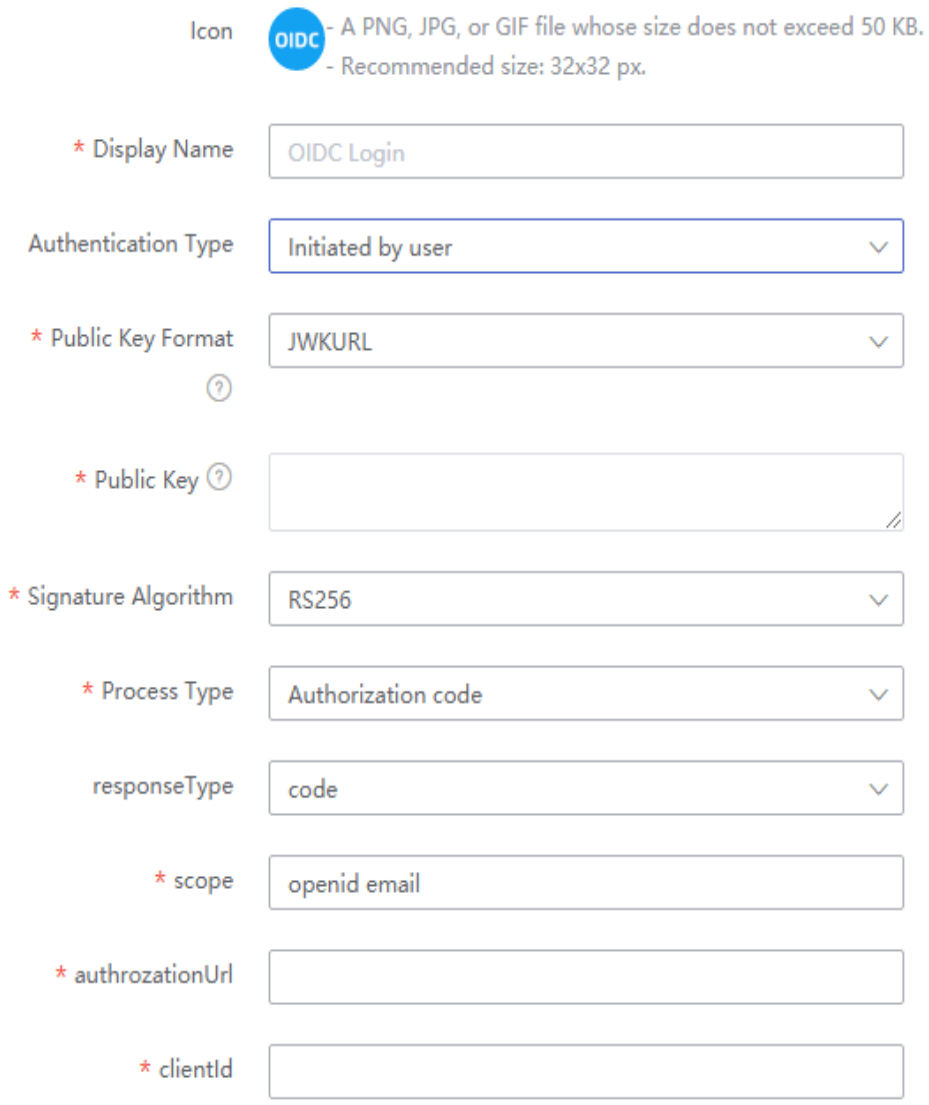
Figure 4-12 Clicking OIDC



Step 3 On the **OIDC Authentication Providers** page, click **Add Authentication Provider** in the upper right corner and set the parameters required.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-13 Configuring parameters



 Copyright © Huawei Technologies Co., Ltd.

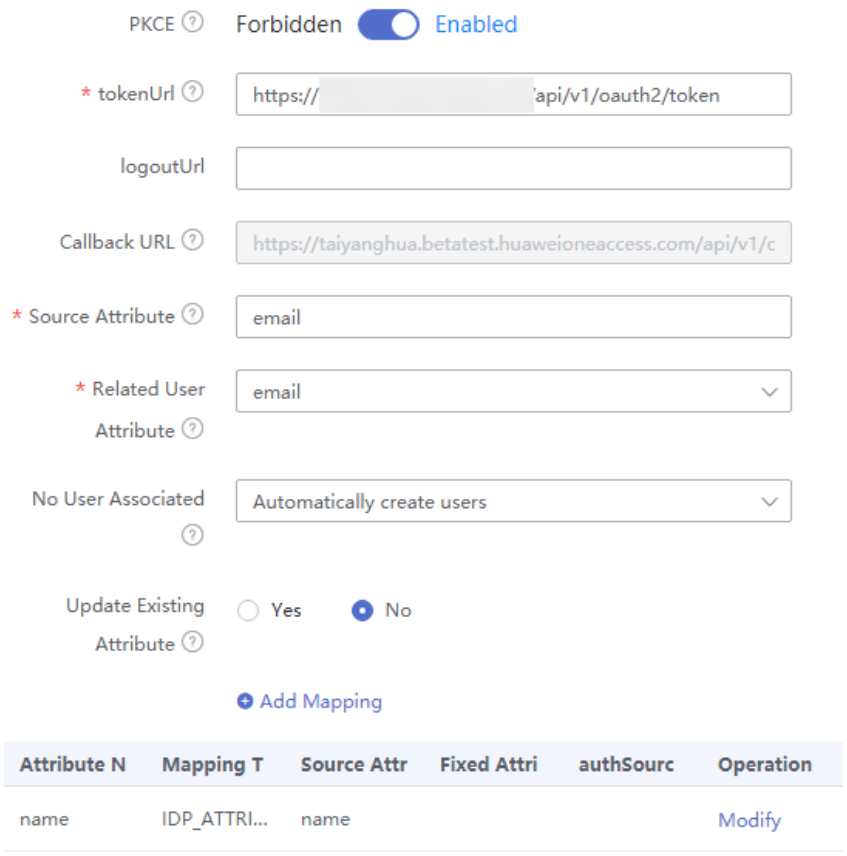


Table 4-3 Configuration parameters

Parameter	Mandatory	Description
Icon	No	Upload a PNG, JPG, or GIF image whose size does not exceed 50 KB. The recommended size is 32 x 32 pixels.
Display Name	Yes	Display name of the authentication provider, for example, **OpenID Connect**.
Authentication Type	Yes	User authentication type. Select **Initiated by user**. **NOTE** • The authentication type cannot be changed once specified. • If authentication is initiated from the application side, select **Initiated by authentication provider**.
Public Key Format	Yes	Select a public key format based on the application.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
Public Key	Yes	Obtain the public key displayed in **jwks_uri** of OIDC or from the authentication provider administrator. The public key must match the selected public key format. • If the public key format is **JWKURL**, the public key is **https://***{Okta domain name}***/oauth2/v1/keys**. • If the public key format is **JSON**, the public key is the value in **https://***{Okta domain name}***/oauth2/v1/keys**.
Signature Algorithm	Yes	The default value is **RS256**.
Audience	Yes	If **Authentication Type** is set to **Initiated by authentication provider**, set this parameter to the value of **Audience** generated for the application created in **Step 1**.
Process Type	Yes	Select a process type based on the application configuration. For example, select **Authorization code** from the drop-down list.
response Type	Yes	The default value is **code**.
scope	Yes	Corresponds to the value of **scopes** of the OIDC authentication provider. The value of this parameter must contain **openid**. For example, **openid email**.
authrozationUrl	Yes	Corresponds to the value of **EMBED LINK** of the OIDC authentication provider.
clientId	Yes	Corresponds to the value of **Client ID** of the OIDC authentication provider.
PKCE	Yes	By default, this option is disabled. If **Authentication Type** is set to **Initiated by user**, enable this option.
tokenUrl	Yes	Token address, which you can obtain from token_endpoint of OIDC. The format is **https://***{Okta domain name}***/api/v1/oauth2/token**.
logoutUrl	No	Global logout address of the application, which you can obtain from the application.
Callback URL	Yes	Corresponds to the **Login redirect URIs** parameter of the application. The value of this parameter is automatically generated.
Source Attribute	Yes	Unique user attribute on the OIDC authentication provider side. For example, **email**.
Related User Attribute	Yes	OneAccess user attribute that maps the user attribute of the OIDC authentication provider. For example, **email**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
No User Associated	Yes	Operation that will be performed if a user successfully logs in through OIDC authentication but fails to be associated with a system user.

To map other attributes, such as full name, set **No User Associated** to **Automatically create users**, and add the desired mappings. For details, see **Table 4-4**.

Table 4-4 Mapping parameters

Parameter	Description
User Attribute	Attribute (such as full name) in OneAccess that maps to the OIDC application.
Mapping Type	Mode of user attribute mapping between OneAccess and the OIDC application.
Authentication Provider Attribute Name	User attribute in the OIDC application, for example, **name**.

----End

Enabling OIDC Authentication

Step 1 Log in to the administrator portal.

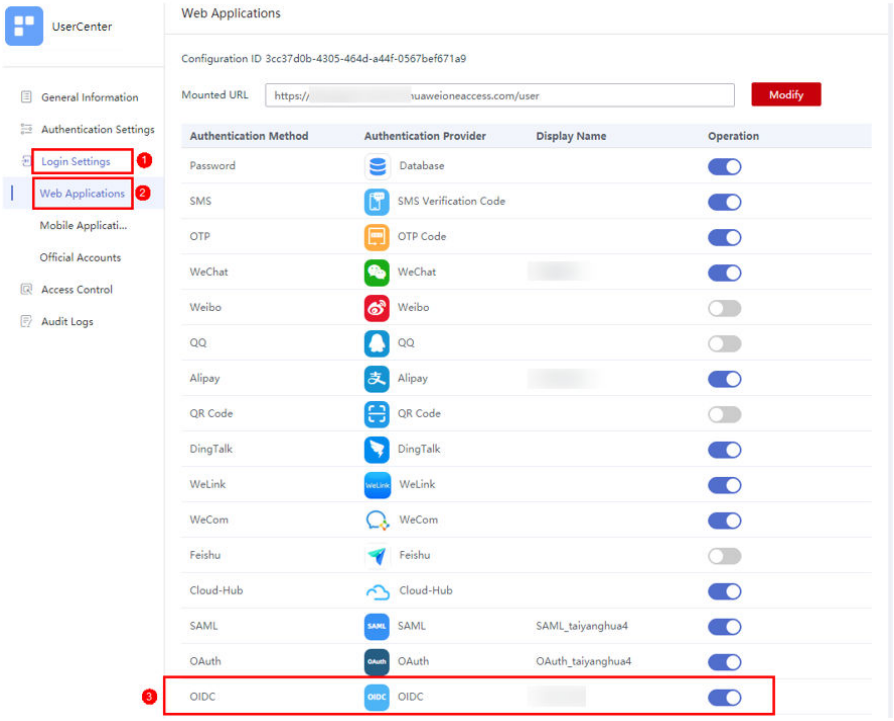
Step 2 In the top navigation pane, choose **Resources** > **Applications**. Then select **UserCenter** in the **Pre-integrated Applications** section.

Step 3 On the application information page, click the application icon.

Step 4 On the application details page, choose **Login Settings** > **Web Applications**, enable OIDC authentication, and select the authentication provider added in **Adding an OIDC Authentication Provider**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-14 Enabling OIDC authentication

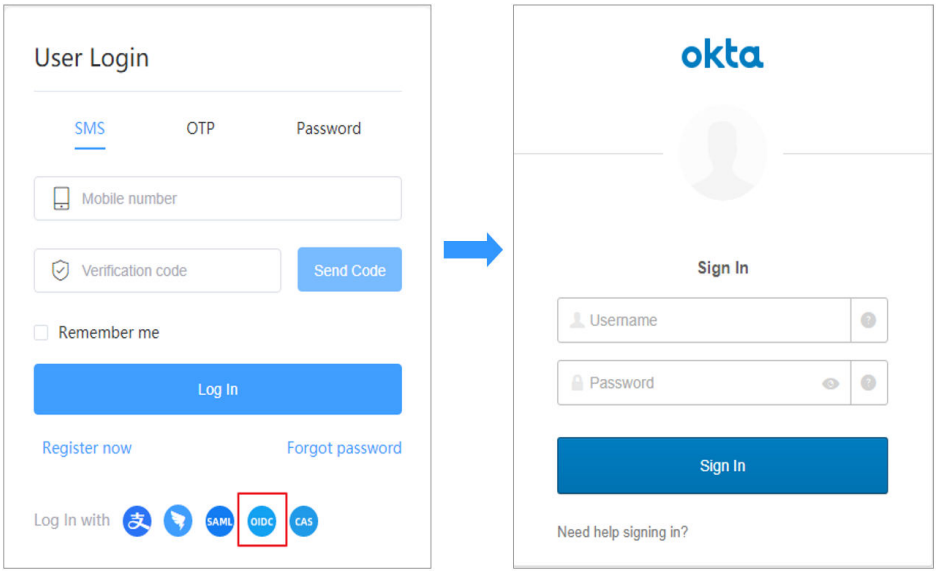


----End

Logging In to the User Portal Through OIDC Authentication

Step 1 Go to the user portal login page, select **OIDC**, enter the username and password of the user authorized in **Step 3**, and click **Log In**.

Figure 4-15 Selecting OIDC



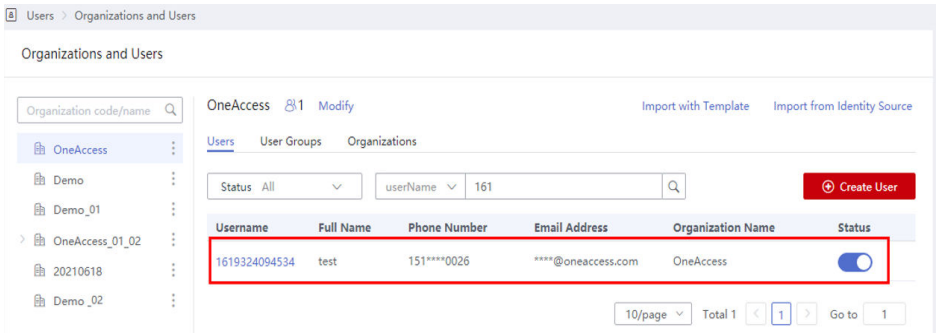
Step 2 After login, go to the administrator portal, choose **Users** > **Organizations and Users**, and view the automatically created user.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- To automatically create a new user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 4-3**.
- If the user attribute **email** is unique, users automatically created in the preceding scenario belong to the first root organization in OneAccess by default.

Figure 4-16 Viewing users



----End

4.3 CAS Authentication

Introduction

CAS is an HTTP2- and HTTP3-based protocol which requires that each component be accessed through a specific URL. You can configure OneAccess as a service provider using the CAS protocol to enable user accounts of third-party applications to access OneAccess. CAS 1.0, CAS 2.0, and CAS 3.0 are supported.

The CAS protocol involves two entities: CAS client and CAS server. They exchange information through users' browsers. For example, a CAS client returns a redirect message containing parameters and forwards the message to the CAS server. If the login authentication is successful, the CAS server returns an XML response containing the user information to the CAS client. After authenticating the user information, the CAS client returns the requested resource to the user.

- CAS client: resource provider, for example, third-party applications.
- CAS server: identity authentication provider. For example, OneAccess can be considered as an identity authentication provider.

This section describes how to integrate a third-party authentication provider with OneAccess through CAS.

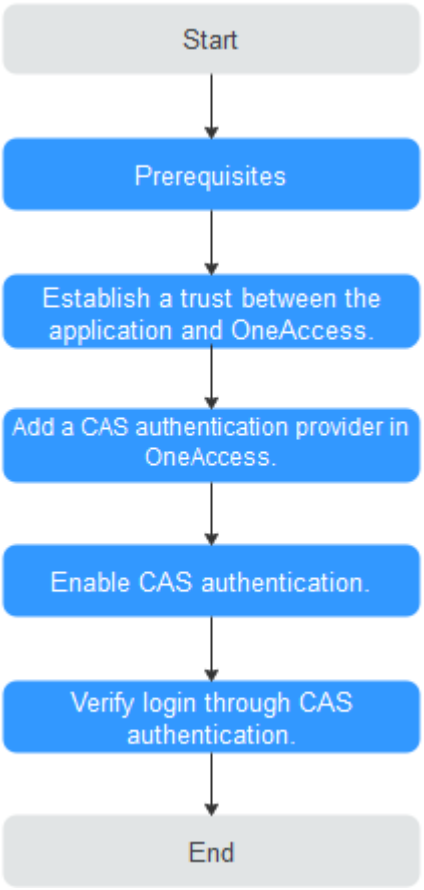
NOTE

The procedure for accessing the user portal on a PC is used for illustration. Configure an application that meets your service requirements.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process

Figure 4-17 Configuration process



Prerequisites

You have permissions to access the administrator portal.

Establishing a Trust Between the Application and OneAccess

Configure authorization information for OneAccess in the application to establish a trust on OneAccess.

Step 1 Obtain the authentication information in OneAccess.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Settings** > **Server Settings**. Then click **CAS**.
3. On the **CAS** page, view the authentication address.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-18 Viewing CAS configurations

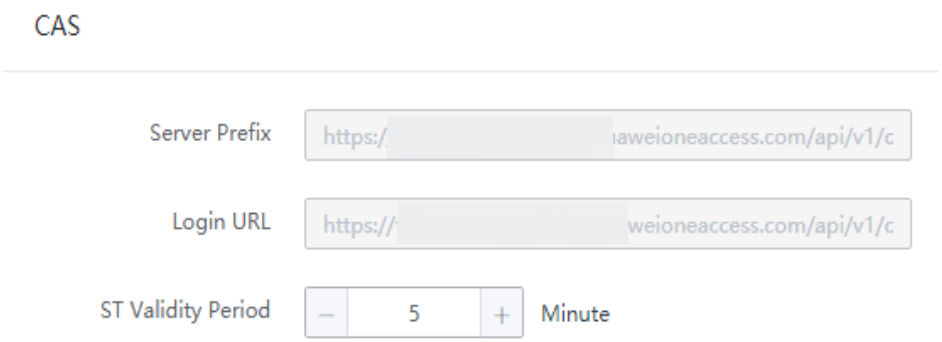


Table 4-5 Configuration parameters

Parameter	Description
Server Prefix	Prefix of the CAS server URL. The prefix is automatically generated and cannot be changed.
Login URL	Request authorization URL of the CAS server. The URL is automatically generated and cannot be changed.
ST Validity Period	Validity period of a returned ST. Set a validity period from 3 to 15 minutes.

Step 2 Obtain the service address in OneAccess. For details, see **Table 4-6**.

Step 3 Configure the preceding information in the application. For details, see the application provider's documentation.

Step 4 Obtain the authorization information of the application. For details, see the application provider's documentation.

----End

Adding a CAS Authentication Provider

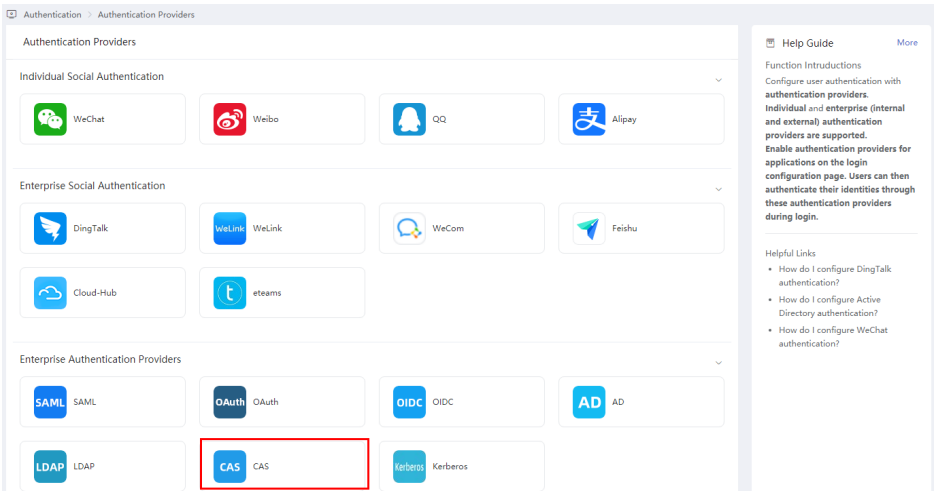
Add a CAS authentication provider and configure the application information in OneAccess.

Step 1 Log in to the administrator portal.

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

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-19 Clicking CAS



Step 3 On the **CAS Authentication Providers** page, click **Add Authentication Provider** in the upper right corner and set the parameters required.

Table 4-6 Configuration parameters

Parameter	Mandatory	Description
Icon	No	Upload a PNG, JPG, or GIF image whose size does not exceed 50 KB. The recommended size is 32 x 32 pixels.
Display Name	Yes	Display name of the authentication provider, for example, **CAS**.
Login Address	Yes	Login URL of the application, which must start with **http** or **https**. For example, **https://***xxx.xxx.xxx***/login**.
Logout Address	Yes	Logout URL of the application, which must start with **http** or **https**. For example, **https://***xxx.xxx.xxx***/logout**.
Validation Address	Yes	Validation address of the application, which must start with **http** or **https**. The validation address varies depending on the protocol version. Validation address for CAS 1.0: **https://***xxx.xxx.xxx***/validate**. Validation address for CAS 2.0: **https://***xxx.xxx.xxx***/serviceValidate**. Validation address for CAS 3.0: **https://***xxx.xxx.xxx***/p3/serviceValidate**.
Request Type	Yes	HTTP request initiation mode. The options include **GET** and **POST**.
Server Address	Yes	The value is generated by the system and cannot be modified. Obtain this value when configuring the application.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
CAS Protocol Version	Yes	Protocol version supported by the application. CAS 1.0 and CAS 2.0 do not support the transfer of user attribute values.
Authentication Provider Attribute	Yes	User attribute returned upon successful authentication by the CAS server. This attribute must be the same as that of the application.
Related User Attribute	Yes	OneAccess user attribute that maps the user attribute of the CAS authentication provider. For example, **userName**.
No User Associated	Yes	Operation that will be performed if a user successfully logs in through CAS authentication but fails to be associated with a system user.

To map other attributes, such as email, set **No User Associated** to **Automatically create users**, and add the desired mappings. For details, see **Table 4-7**.

Table 4-7 Mapping parameters

Parameter	Description
User Attribute	Attribute in OneAccess that maps to the CAS application. For example, **mobile**.
Mapping Type	Mode of user attribute mapping between OneAccess and the CAS application.
Authentication Provider Attribute Name	User attribute in the CAS application. For details, see the application's configurations.

----End

Enabling CAS Authentication

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Resources** > **Applications**. Then select **UserCenter** in the **Pre-integrated Applications** section.

Step 3 On the application information page, click the application icon.

 Copyright © Huawei Technologies Co., Ltd.

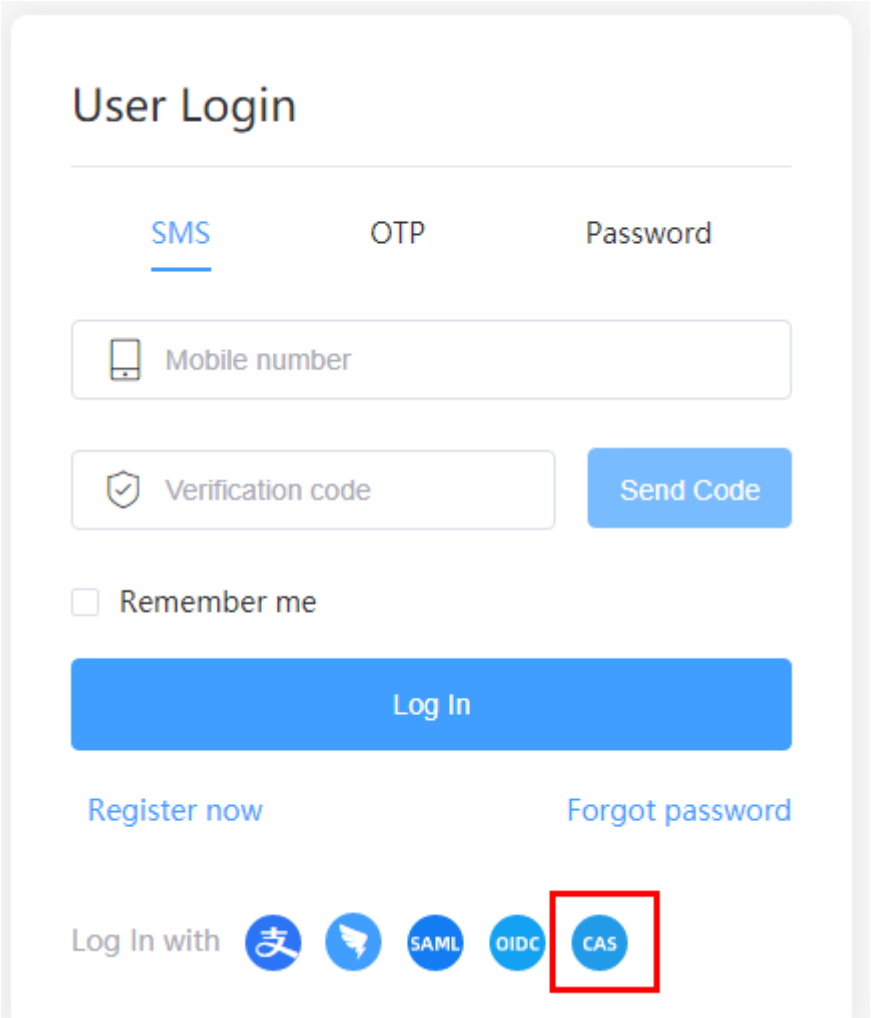
Step 4 On the application details page, choose **Login Settings** > **Web Applications**, enable CAS authentication, and select the authentication provider added in **Adding a CAS Authentication Provider**.

----End

Logging In to the User Portal Through CAS Authentication

Step 1 Go to the user portal login page, select **CAS**, enter an account and password of the application, and click **Log In**.

Figure 4-20 Selecting CAS



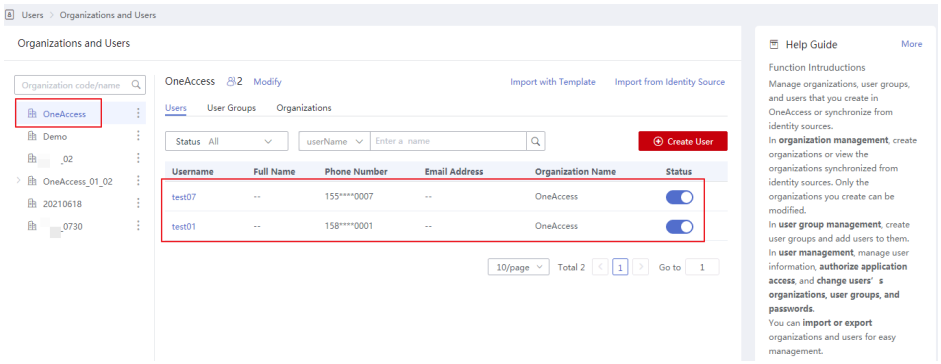
Step 2 After login, go to the administrator portal, choose **Users** > **Organizations and Users**, and view the automatically created user.

NOTE

- To automatically create a new user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 4-6**.
- By default, users automatically created in the preceding scenario belong to the first root organization in OneAccess.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-21 Viewing users



----End

4.4 OAuth Authentication

OAuth is an open standard that allows users to authorize third-party applications to access their information stored on a specific resource server without sharing usernames and passwords with the third-party applications.

This section describes how to integrate a third-party authentication provider with OneAccess through OAuth.

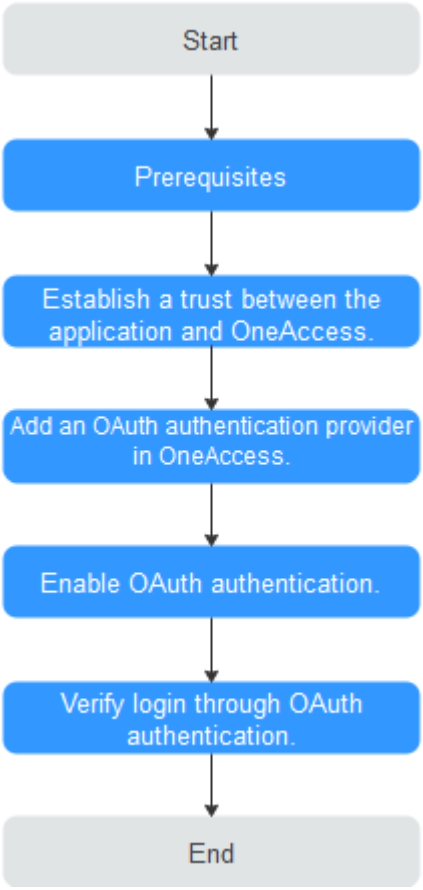
NOTE

The procedure for accessing the user portal on a PC is used for illustration. Select and configure an application that meets your service requirements.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process

Figure 4-22 Configuration process



Prerequisites

You have permissions to access the administrator portal.

Establishing a Trust Between the Application and OneAccess

Configure authorization information for OneAccess in the application to establish a trust on OneAccess.

Step 1 Obtain the authentication information in OneAccess.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Settings** > **Server Settings**. Then click **OIDC**.
3. On the **OIDC** page, view the authentication address.
4. Click **OIDC Discovery** in the upper right and view the authentication parameters.

Step 2 Obtain the callback address in OneAccess. For details, see **Table 4-8**.

Step 3 Configure the preceding information in the application. For details, see the application provider's documentation.

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Obtain the authorization information of the application. For details, see the application provider's documentation.

----End

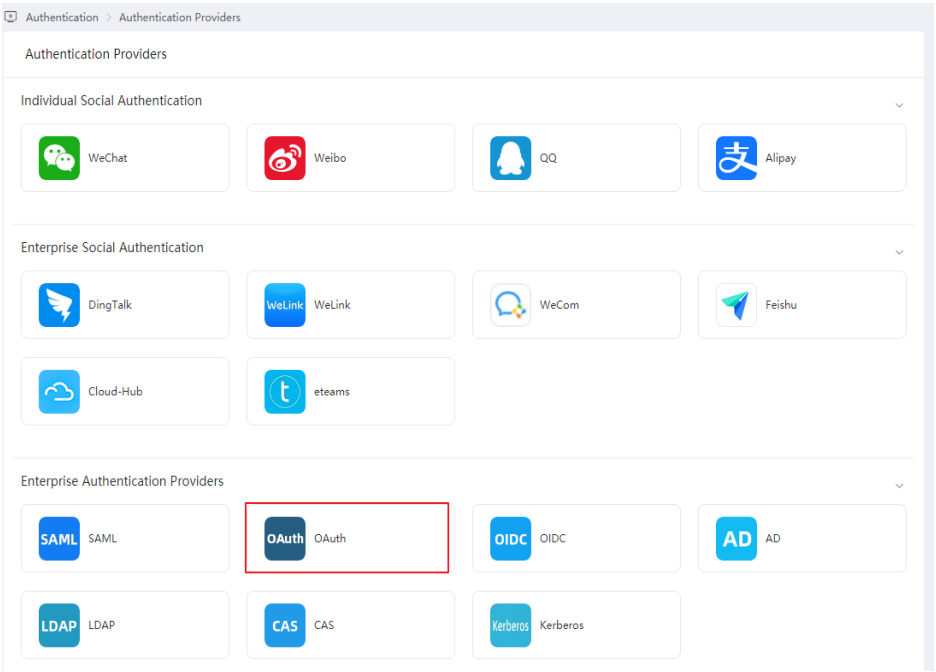
Adding an OAuth Authentication Provider

Add an OAuth authentication provider and configure the application information in OneAccess.

Step 1 Log in to the administrator portal.

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

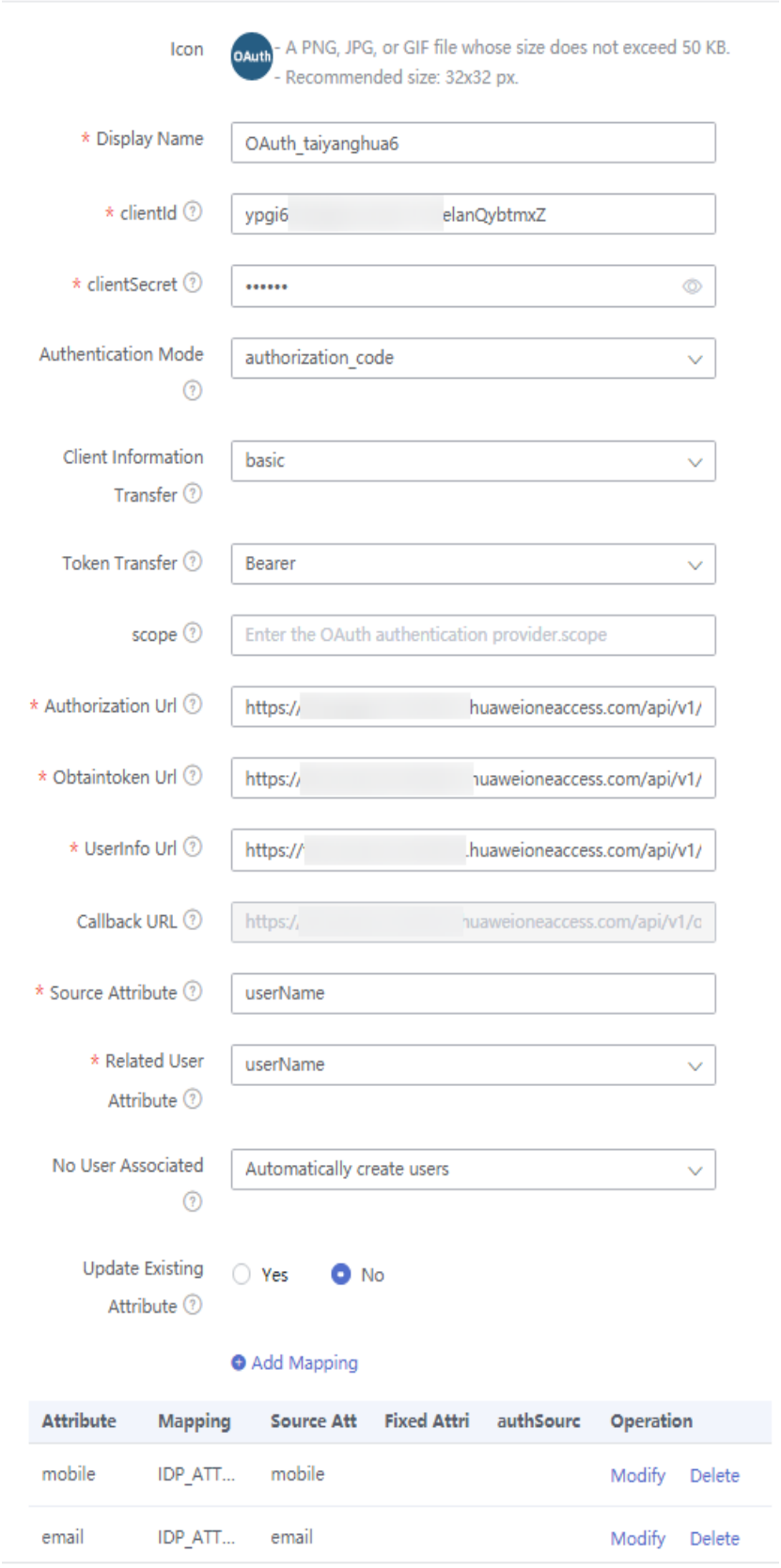
Figure 4-23 OAuth



Step 3 On the **OAuth Authentication Providers** page, click **Add Authentication Provider** in the upper right corner and set the parameters required.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-24 Configuring parameters



 Copyright © Huawei Technologies Co., Ltd.

Table 4-8 Configuration parameters

Parameter	Mandatory	Description
Icon	No	Upload a PNG, JPG, or GIF image whose size does not exceed 50 KB. The recommended size is 32 x 32 pixels.
Display Name	Yes	Display name of the authentication provider, for example, **OAuth**.
clientId	Yes	Client ID of the application. Obtain the value from the application.
clientSecret	Yes	Client secret of the application. Obtain the value from the application.
Authentication Mode	Yes	Default value: **authorization_code**.
Client Information Transfer	Yes	Options: **basic** and **post**.
Token Transfer	Yes	Default value: **Bearer**.
scope	No	Authorization scope. Separate multiple values with commas (,).
Authorization Url	Yes	Authentication URL of the application. Obtain the value from the application.
Obtaintoken Url	Yes	URL for obtaining a token. Obtain the value from the application.
UserInfo Url	Yes	URL for obtaining user information. Obtain the value from the application.
Callback URL	Yes	The value is generated by the system and cannot be modified. You can obtain this value when configuring the application.
Source Attribute	Yes	User attribute returned upon successful authentication by the server. This attribute must be the same as that of the application.
Related User Attribute	Yes	OneAccess user attribute that maps the user attribute of the OAuth authentication provider. For example, username.
No User Associated	Yes	Operation that will be performed if a user successfully logs in through OAuth authentication but fails to be associated with a system user.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
Update Existing Attribute	Yes	Disabled by default. Determine whether to update the existing user attribute value when a user logs in successfully through the authentication provider and is associated with a system user.

To map other attributes, such as full name, set **No User Associated** to **Automatically create users**, and add the desired mappings. For details, see **Table 4-9**.

Table 4-9 Mapping parameters

Parameter	Description
User Attribute	Attribute (such as full name) in OneAccess that maps to the OAuth application.
Mapping Type	Mode of user attribute mapping between OneAccess and the OAuth application.
Authentication Provider Attribute Name	User attribute in the OAuth application. For details, see the application's configurations.

----End

Enabling OAuth Authentication

Step 1 Log in to the administrator portal.

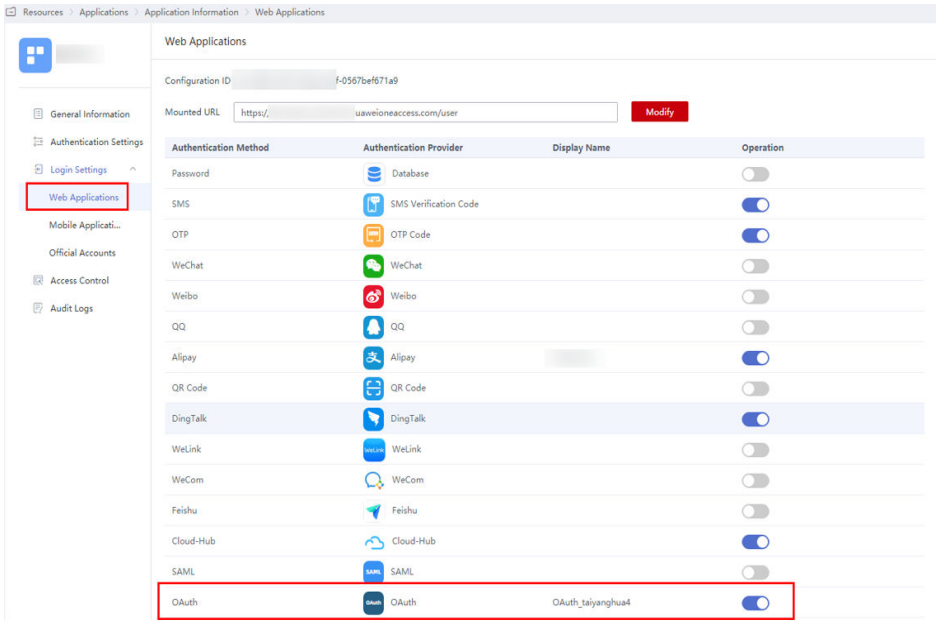
Step 2 In the top navigation pane, choose **Resources** > **Applications**. Then select **UserCenter** in the **Pre-integrated Applications** section.

Step 3 On the application information page, click the application icon.

Step 4 On the application details page, choose **Login Settings** > **Web Applications**, enable OAuth authentication, and select the authentication provider added in **Adding an OAuth Authentication Provider**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-25 Enabling OAuth authentication



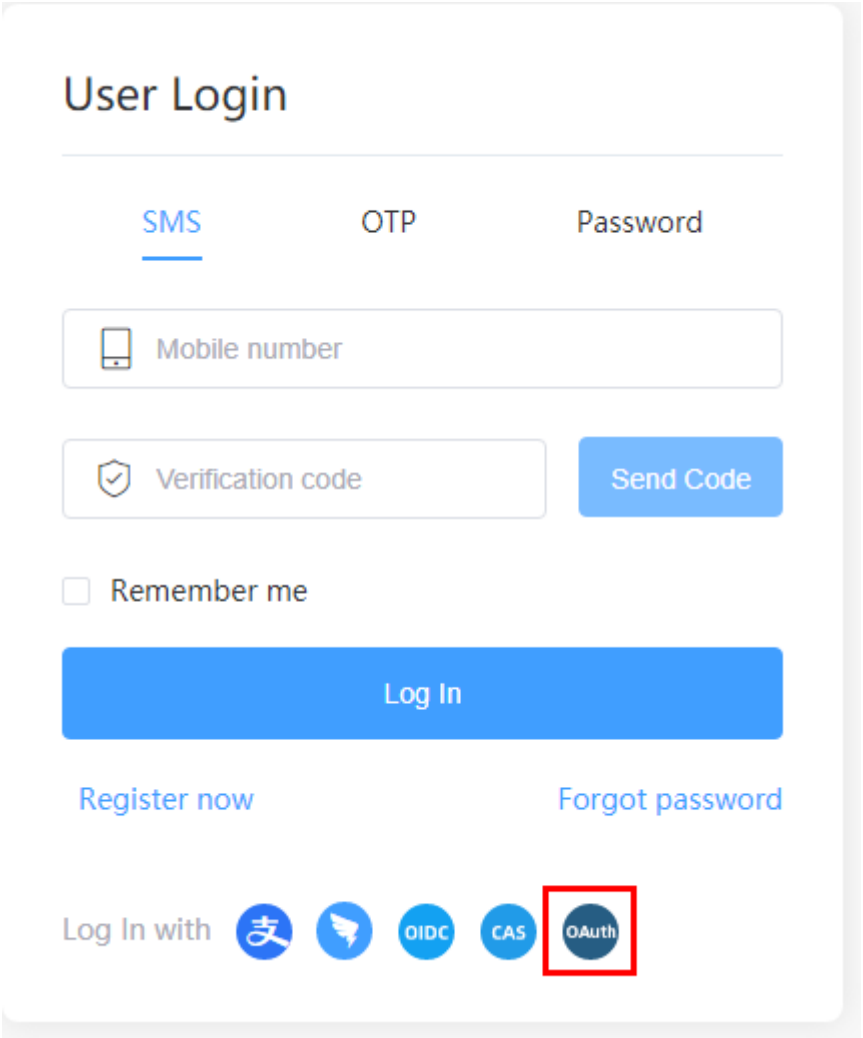
----End

Logging In to the User Portal Through OAuth Authentication

Step 1 Go to the user portal login page, select **OAuth**, enter an account and password of the application, and click **Log In**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-26 Selecting OAuth



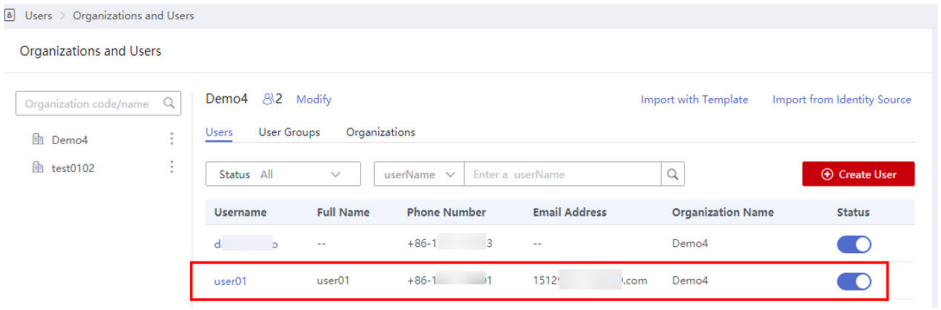
Step 2 After login, go to the administrator portal, choose **Users** > **Organizations and Users**, and view the automatically created user.

NOTE

- To automatically create a new user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 4-9**.
- By default, users automatically created in the preceding scenario belong to the first root organization in OneAccess.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-27 Viewing users



----End

4.5 AD Authentication

OneAccess supports user identity authentication and permission control using AD. AD is a database that stores network objects, allowing administrators and users to search for required information.

This section describes how to integrate AD with OneAccess.

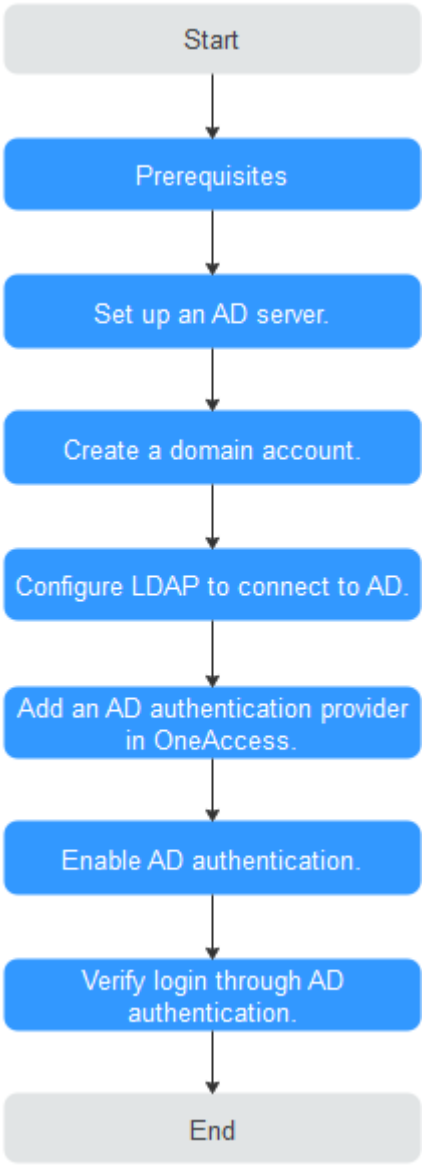
NOTE

The procedure for accessing the user portal on a PC is used for illustration. Select and configure an application that meets your service requirements.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process

Figure 4-28 Configuration process



Prerequisites

You have permissions to access the administrator portal.

Setting Up an AD Server

Windows Server 2012 R2 is used as an example to describe how to set up a domain server.

Step 1 In Server Manager, choose **Manage** > **Add Roles and Features** in the upper right.

Step 2 In the **Add Roles and Features Wizard** dialog box, click **Next** until the **Select server roles** page is displayed. Select **Active Directory Domain Services** and click **Add Features** in the displayed box.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Click **Next** until the **Confirm installation selections** page is displayed. Click **Install** to start the role installation process.

Step 4 After the installation is complete, click the yellow triangle icon displayed in the upper right, and click **Promote this server to a domain controller**. The **Active Directory Domain Services Configuration Wizard** window is displayed.

Step 5 On the **Deployment Configuration** page, select **Add a new forest** and set a domain name, such as **oneaccess.com**.

Step 6 Click **Next**. On the displayed page, enter the DSRM password of a non-domain user.

Step 7 Click **Next** until the **Prerequisites Check** page is displayed. Click **Install**. After the installation is complete, the server is automatically restarted.

----End

Creating a Domain Account

Step 1 Choose **Tools** > **Active Directory Users and Computers** in the upper right corner.

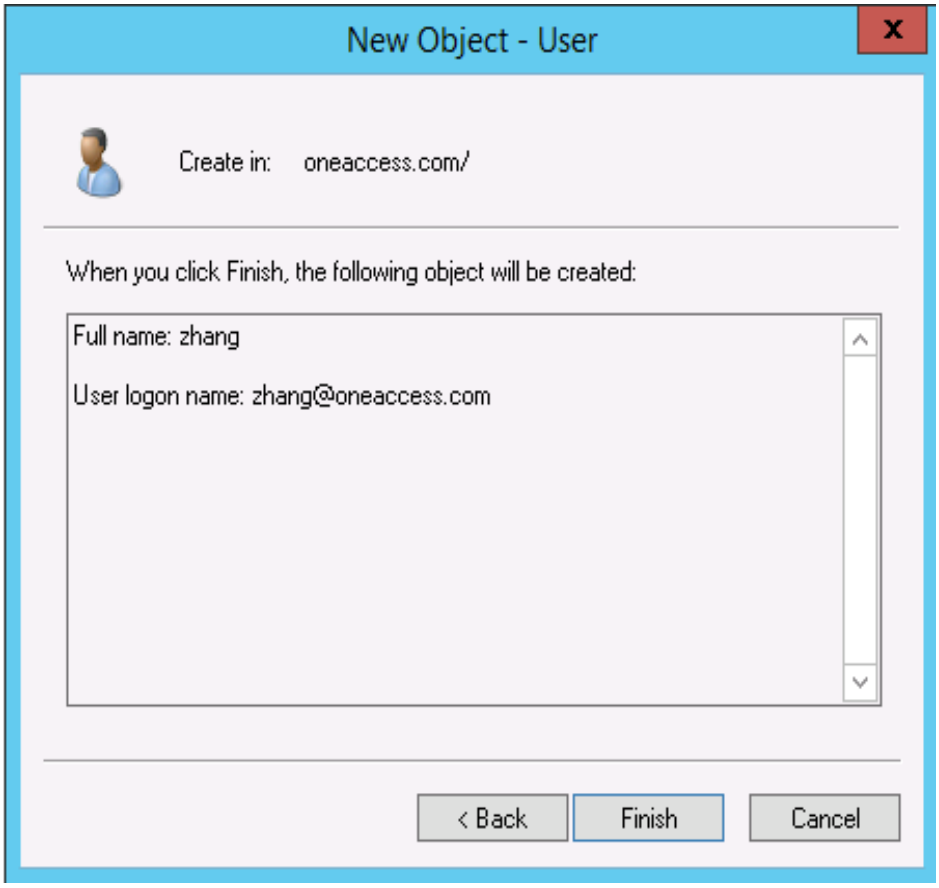
Step 2 Right-click the target domain, choose **New** > **User**, enter a username, and click **Next**.

Step 3 Set **Full name** and **User logon name** and click **Next**. For example, **john@oneaccess.com**.

Step 4 Enter a password for the domain account and enter the password again. Deselect all check boxes. (You do not need to change the password at the first login.)

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-29 Creating an object



----End

Configuring LDAP to Connect to AD

Step 1 Download and install ApacheDirectoryStudio, an LDAP client.

Step 2 Choose **LDAP** > **New Connection** and set the connection parameters. If the connection is successful, user and organization information in the AD is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-30 Creating a connection

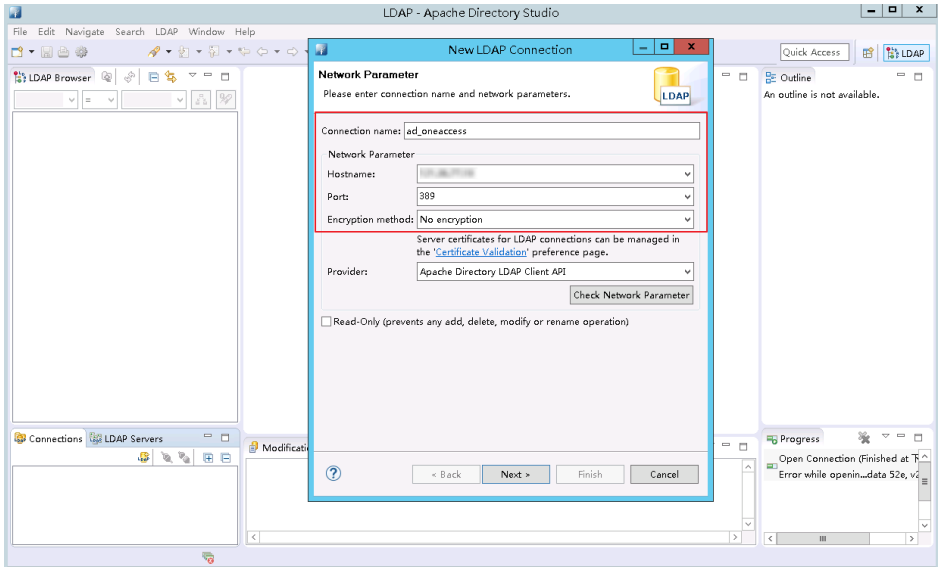
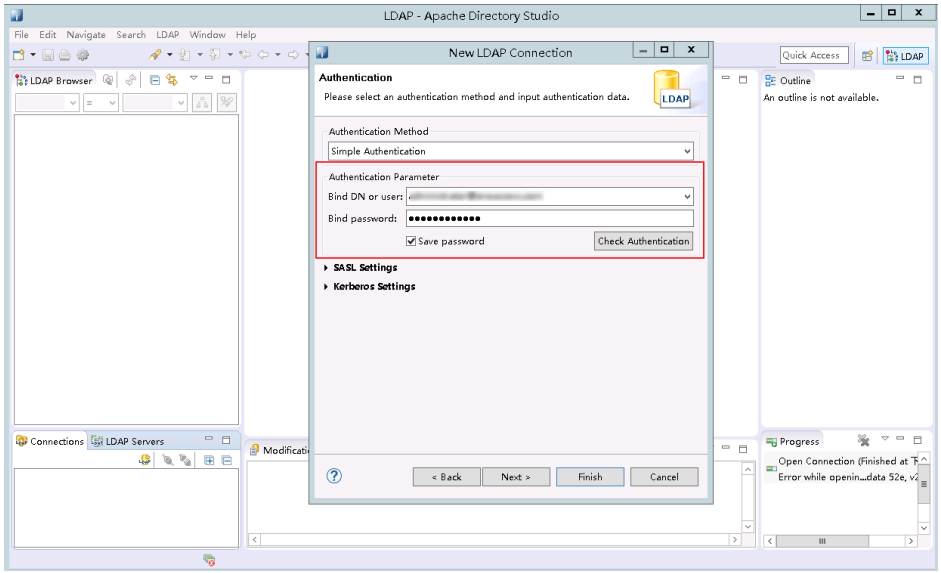
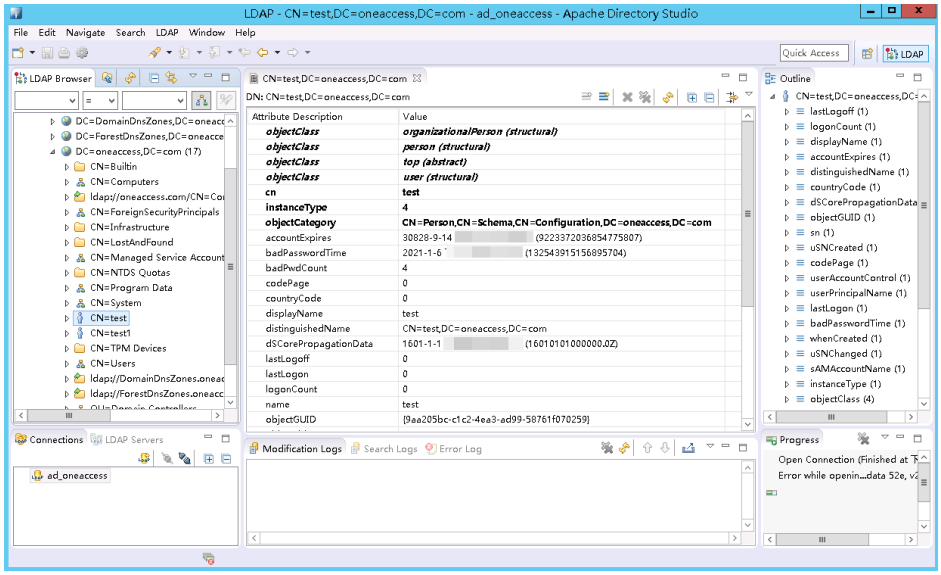


Figure 4-31 Configuring parameters



 Copyright © Huawei Technologies Co., Ltd.

Figure 4-32 Viewing data



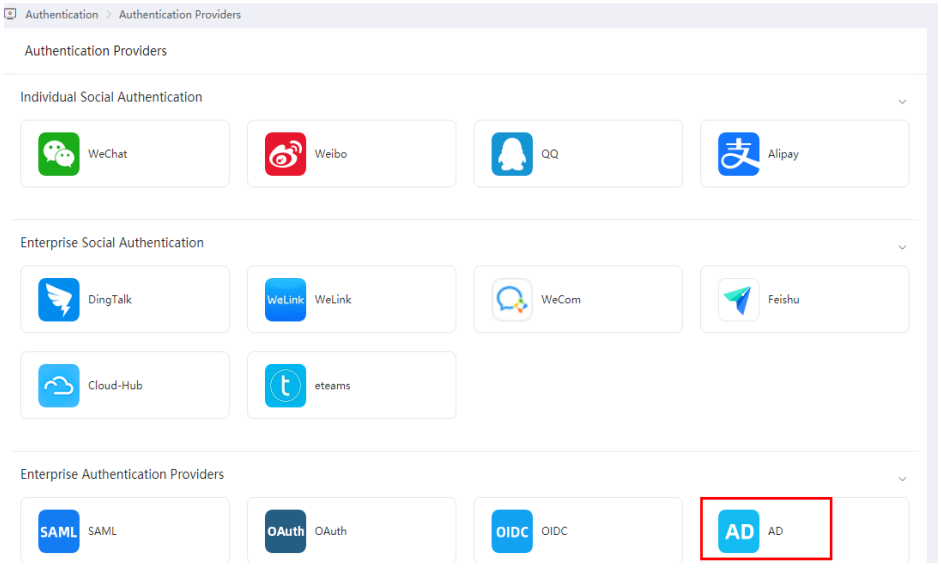
----End

Adding an AD Authentication Provider

Step 1 Log in to the administrator portal.

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

Figure 4-33 Clicking AD



Step 3 On the **AD Authentication Providers** page, click **Add Authentication Provider** in the upper right corner and set the parameters required.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-34 Configuring parameters

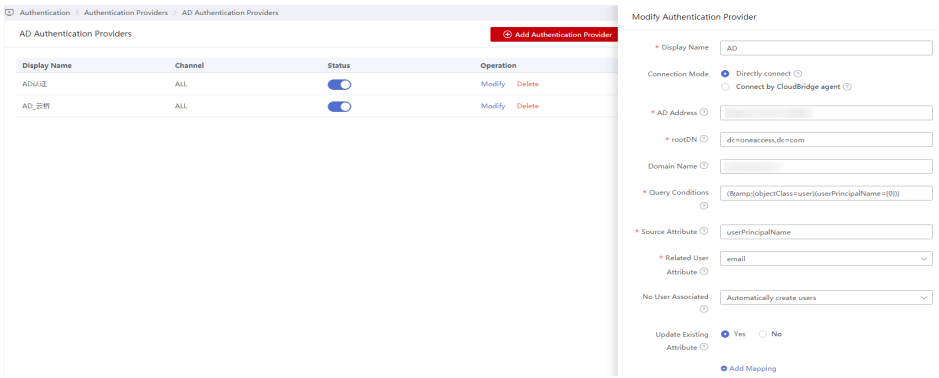


Table 4-10 Configuration parameters

Parameter	Description
Display Name	(Required) Display name of the authentication provider, for example, **AD**.
AD Address	(Required) Connection address of AD in the format "ldap://*{hostname}*:*{port}*/", where *{hostname}* indicates the AD server address and *{port}* indicates the port. The default port is 389. For details, see **Configuring LDAP to Connect to AD**.
rootDN	(Required) A node of AD used to authenticate users. The format of the value is "dc=,dc=". For details, see **Configuring LDAP to Connect to AD**.
Domain Name	(Optional) Domain name set when the AD server is set up. If this parameter is set, the query condition consists of the "login name + @ + domain name". If this parameter is left blank, the query condition contains only the login name. For details, see **Step 5**.
Query Conditions	(Required) Consists of the object class and user login name. Adjust **userPrincipalName** to meet service requirements. If the placeholder is **{0}**, query is performed based on the username entered by a user during login and the domain name, for example, **mike@companya.cn**. If no domain name exists, the domain name of the authentication provider is used. If the placeholder is **{1}**, query is performed only based on the username entered by a user, for example, **mike**.
Source Attribute	(Required) Attribute of the AD user associated with the user login name. For example, **userPrincipalName**. Obtain the attribute from **Configuring LDAP to Connect to AD**.
Related User Attribute	(Required) User attribute mapped by AD in the system. The user attribute must be a unique text.
No User Associated	(Required) Operation that will be performed if a user logs in successfully but fails to be associated with a system user.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Define more user attributes if needed. The attributes must be unique texts. For details, see **Adding a Custom Attribute**.

----End

Enabling AD Authentication

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Resources** > **Applications**. Then select **UserCenter** in the **Pre-integrated Applications** section.

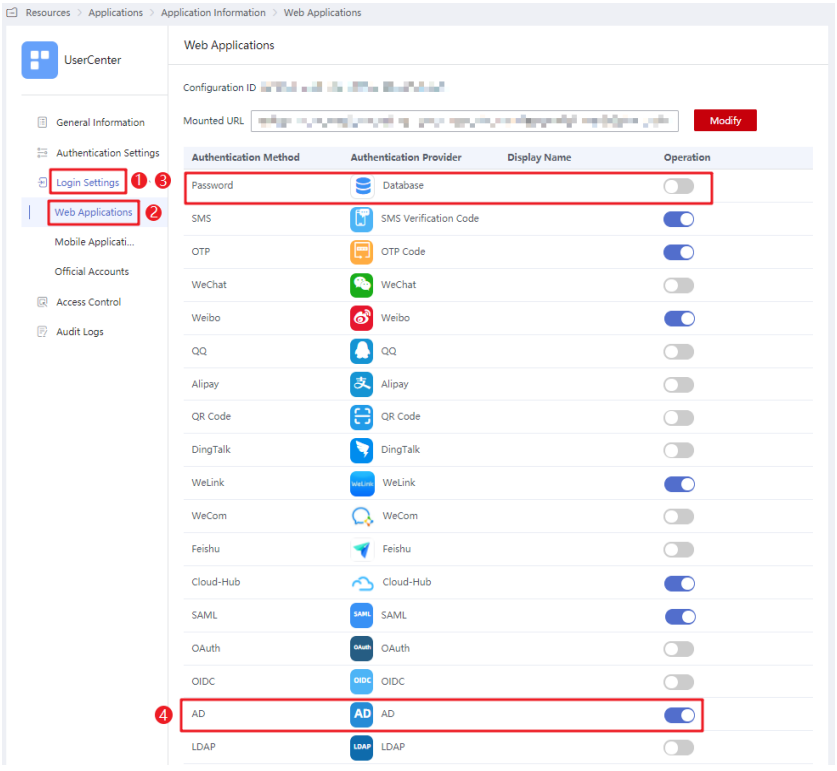
Step 3 On the application information page, click the application icon.

Step 4 On the application details page, choose **Login Settings** > **Web Applications**, enable AD authentication, and select the authentication provider added in **Adding an AD Authentication Provider**.

NOTE

The password text box will be used during AD authentication. To enable AD authentication, **disable database authentication** first.

Figure 4-35 Enabling AD authentication



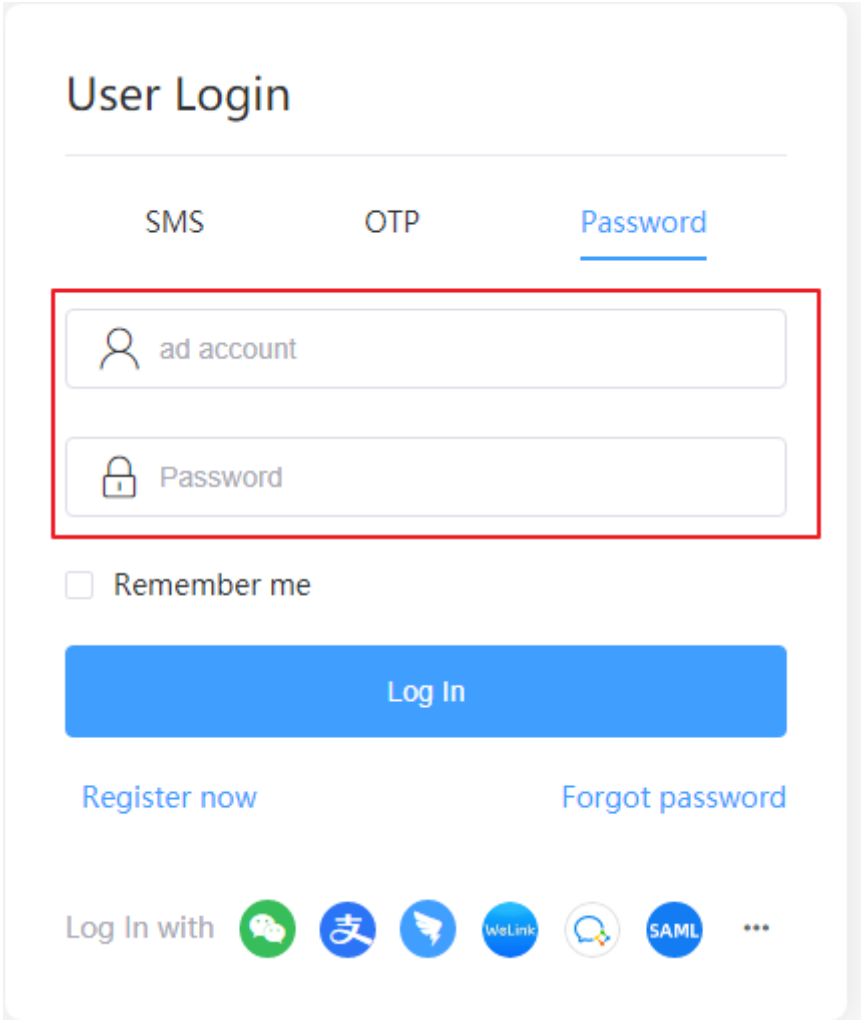
----End

Logging In to the User Portal Through AD Authentication

- On the user portal login page, select **Password**, enter an AD account and password, and click **Log In**.

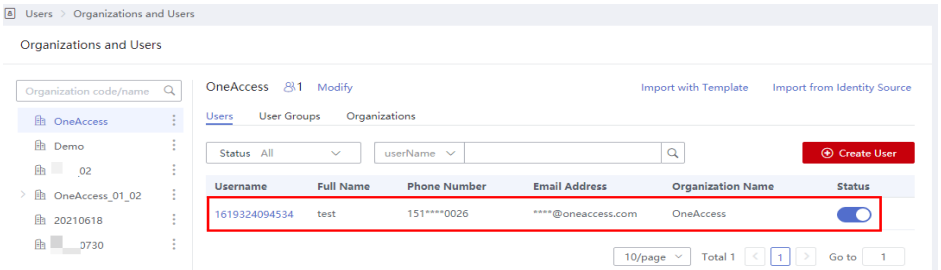
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-36 Selecting Password



- After login, go to the administrator portal, choose **Users** > **Organizations and Users**, and view the automatically created user.

Figure 4-37 Viewing users



- If the AD user is not associated with any OneAccess user and you have set **No User Associated** to **Failed** (see **Figure 4-34**), the login will fail. To ensure successful login, create a user with the same name as the AD user in OneAccess.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-38 Viewing AD users

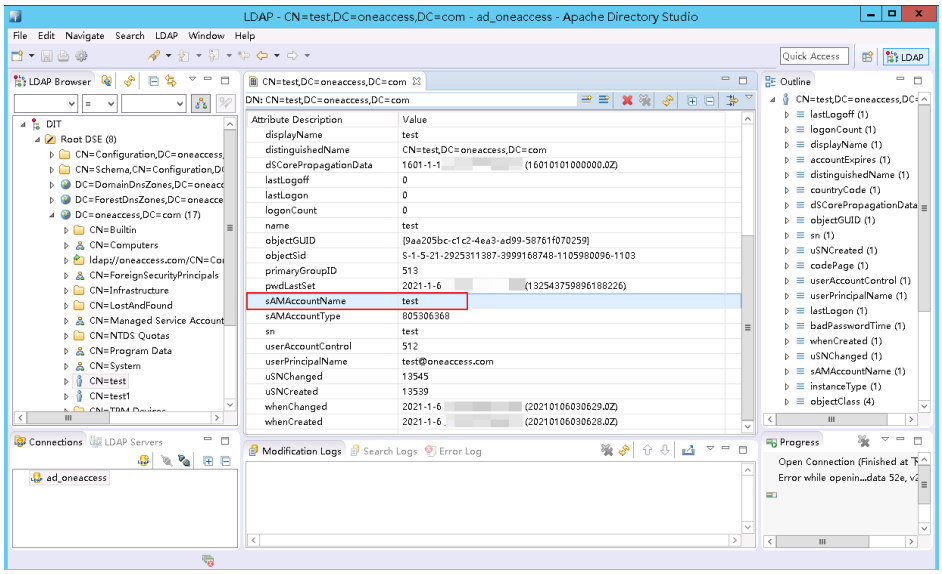
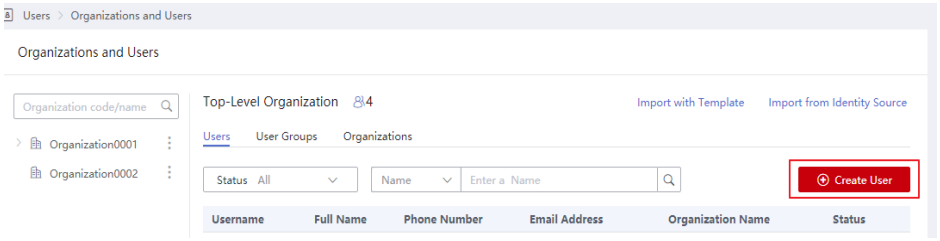
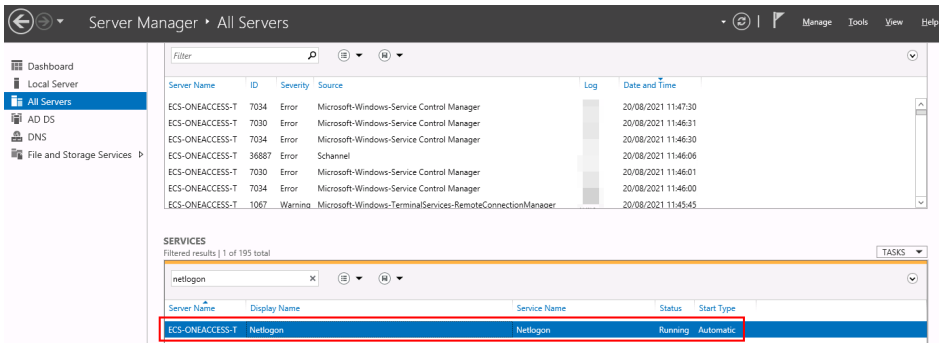


Figure 4-39 Adding users



FAQs

1. When creating a domain account, why am I prompted that the AD cannot be opened because the domain does not exist or cannot be connected?
   - Check whether the Netlogon and DFS services have been started.



   - Run the **net share** command to check whether the sharing is normal.

     If the sharing is abnormal, change the value of **SysvolReady** in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters** to **1**. Run the **net share** command again. The sharing should become normal.
   - For the AD domain, check the logs in the event viewer and use the Dcdiag tool to locate the error.

 Copyright © Huawei Technologies Co., Ltd.

2. Why is **[LDAP: error code 49-80090308:LdapErr:.....AcceptSecurityContext error.data.52e.vece]** displayed during LDAP configuration for AD connection?

   The password or credential is invalid. The correct username format is "*{Username}@{Domain name}*".

4.6 LDAP Authentication

Introduction

OneAccess supports user identity authentication and permission control over LDAP.

- LDAP can be considered a tree-like database that stores user and organization information.
- One of the main application scenarios of LDAP is SSO where users are automatically logged in to internal networks of their company after logging in on a PC for once.

Table 4-11 Terms

Term	Description
OU	Organization unit (OU), which is a container object.
DC	Domain component (dc), which is a part of a domain name. A domain name is divided into several parts.
SN	Short for surname.
CN	Short for common name.
DN	Short for distinguished name. A dn must be unique.
UID	Short for user ID.
RDN	Relative distinguished name (RDN) is similar to the relative path in a file system.

This section describes how to integrate LDAP with OneAccess.

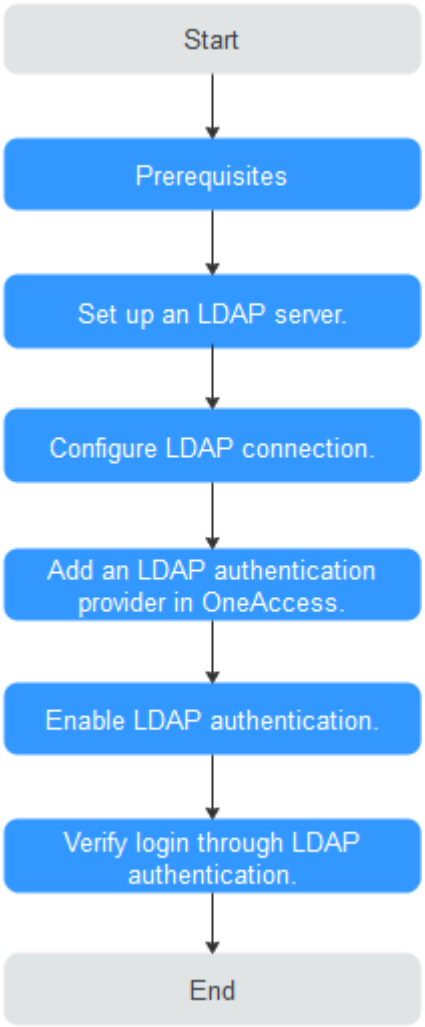
NOTE

The procedure for accessing the user portal on a PC is used for illustration. Select and configure an application that meets your service requirements.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process

Figure 4-40 Configuration process



Prerequisites

You have permissions to access the administrator portal.

Setting Up an LDAP Server

Step 1 Download the Directory Services installation package at the **ForgeRock official website**.

Step 2 Deploy the LDAP service. For details, see the documentation of the ForgeRock platform.

----End

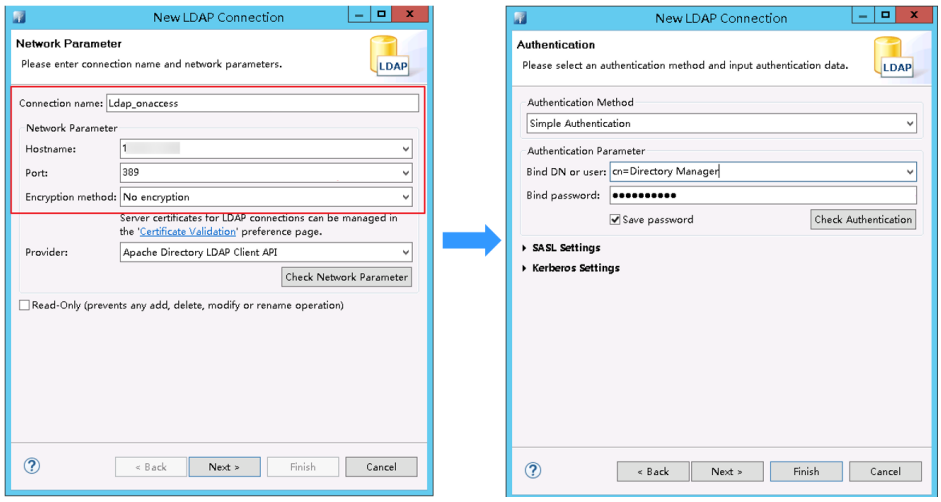
Configuring LDAP Connection

Step 1 Download and install ApacheDirectoryStudio, an LDAP client.

 Copyright © Huawei Technologies Co., Ltd.

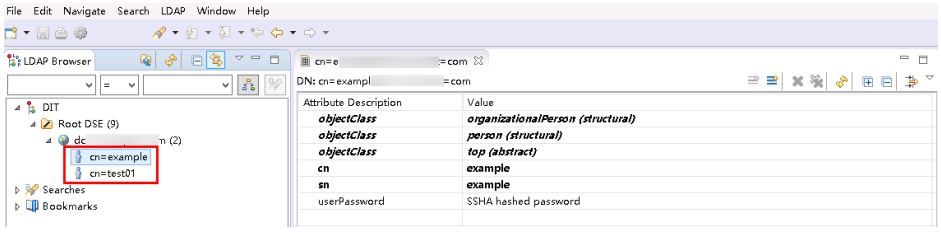
Step 2 Choose **LDAP** > **New Connection** and set the connection parameters.

Figure 4-41 Creating a connection



Step 3 Add an account in LDAP.

Figure 4-42 Viewing users



----End

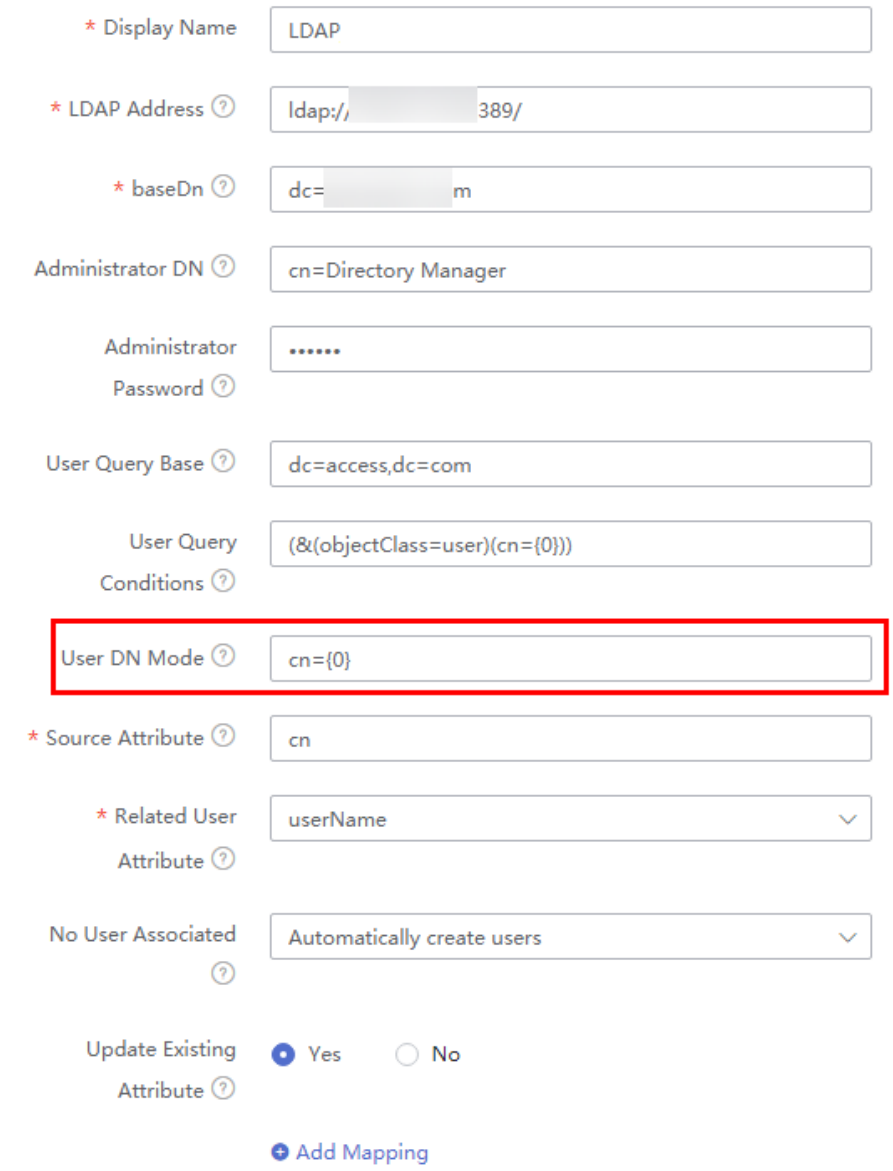
Adding an LDAP Authentication Provider

LDAP has three authentication modes: **DN authentication**, **query authentication**, and **DN and query authentication**.

- DN authentication: Select this authentication mode if you know the user DN rules. For example, uid=**, ou=people, dc=example, dc=com. In this mode, you only need to configure the user DN mode.

 Copyright © Huawei Technologies Co., Ltd.

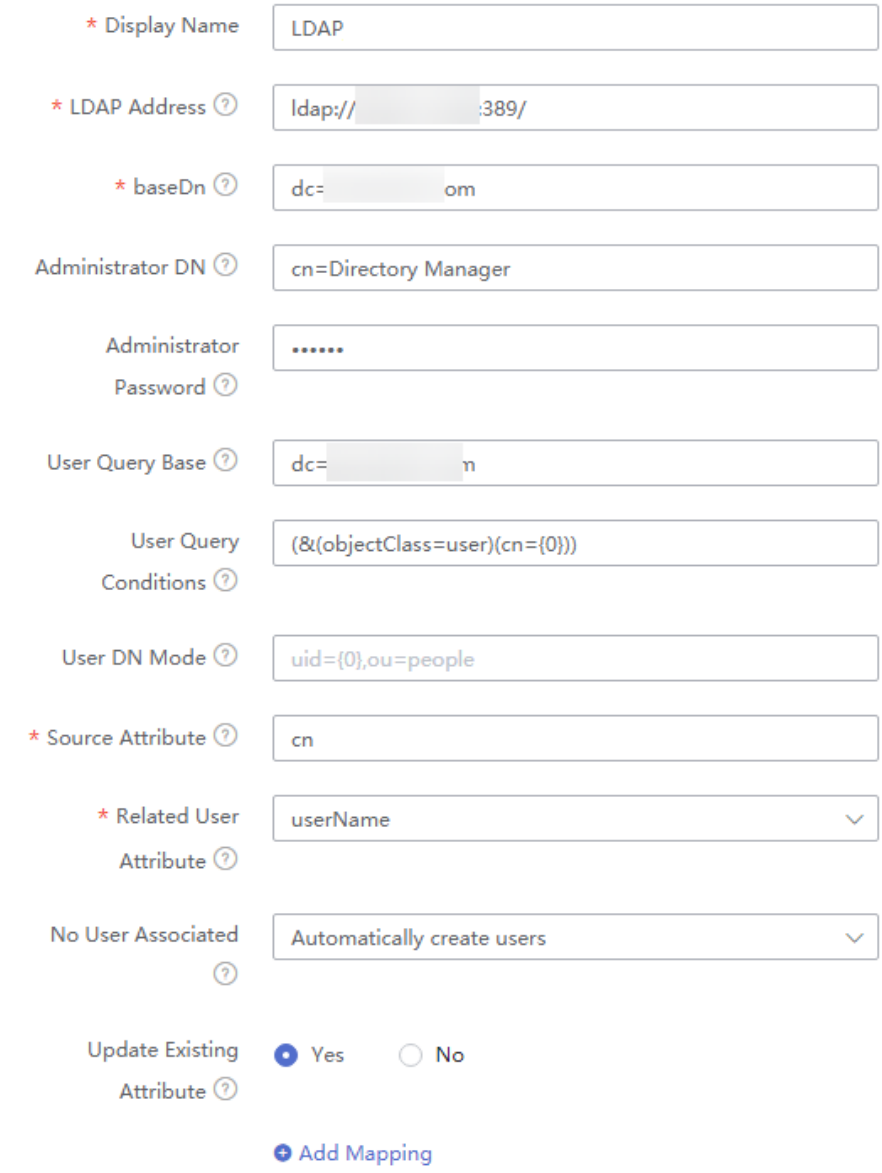
Figure 4-43 DN authentication mode



- Query authentication: When selecting this mode, configure the LDAP administrator account and password and set the query conditions. During authentication, the LDAP administrator account is used to query a user based on the configured conditions and entered username. After a matched user is found, the DN of the user is obtained, and the DN and password of the user are verified in LDAP.

 Copyright © Huawei Technologies Co., Ltd.

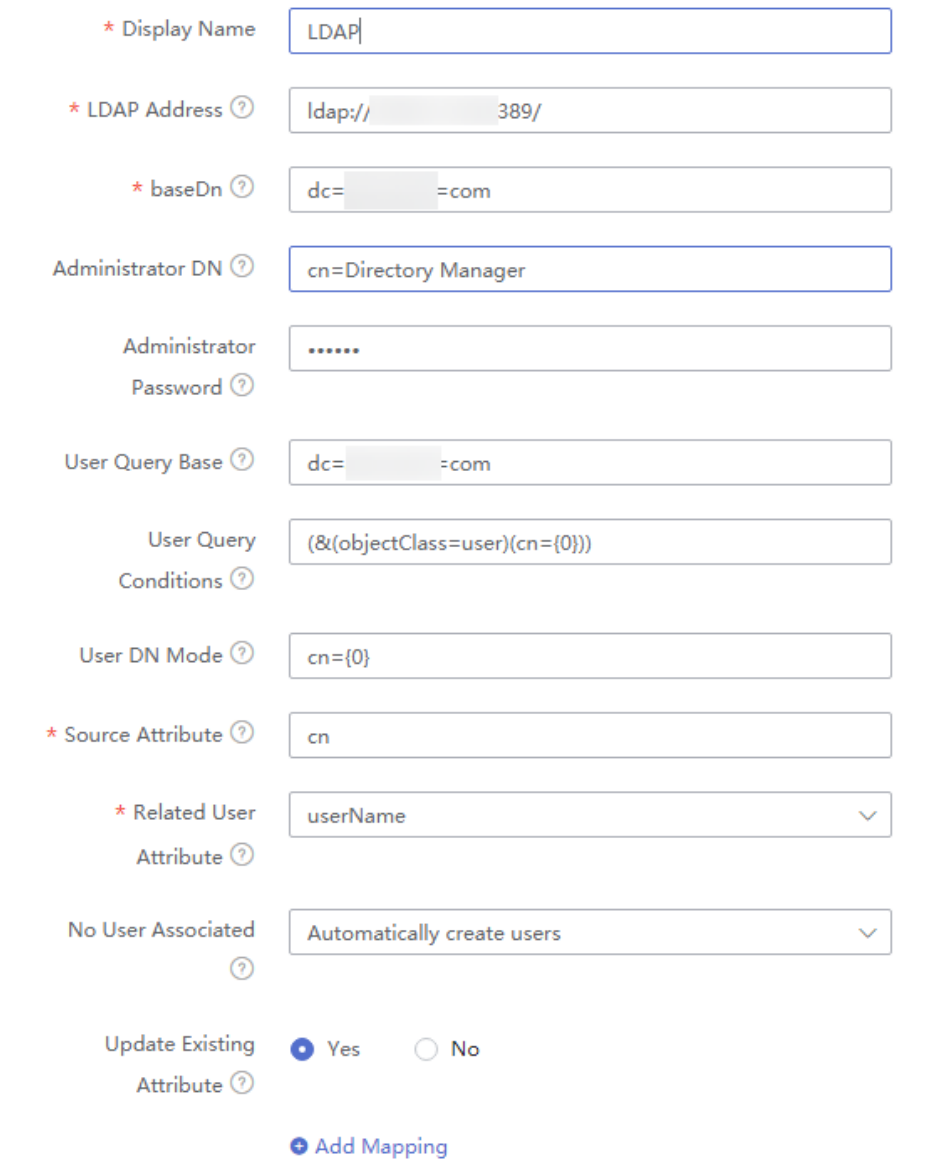
Figure 4-44 Query authentication mode



- DN and query authentication: In this authentication mode, DN takes precedence over the query conditions.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-45 DN and query authentication



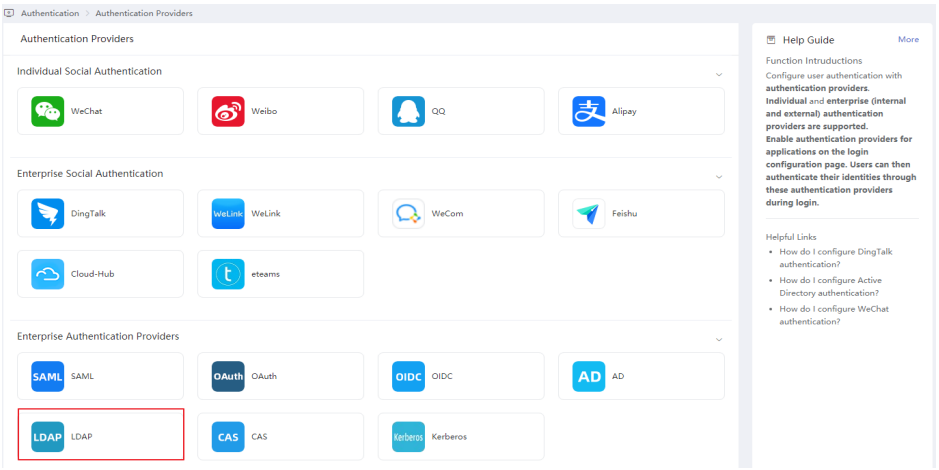
The following is the procedure for configuring DN and query authentication of LDAP.

Step 1 Log in to the administrator portal.

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

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-46 Clicking LDAP



Step 3 On the **LDAP Authentication Providers** page, click **Add Authentication Provider** in the upper right corner and set the parameters required.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-47 Configuring parameters

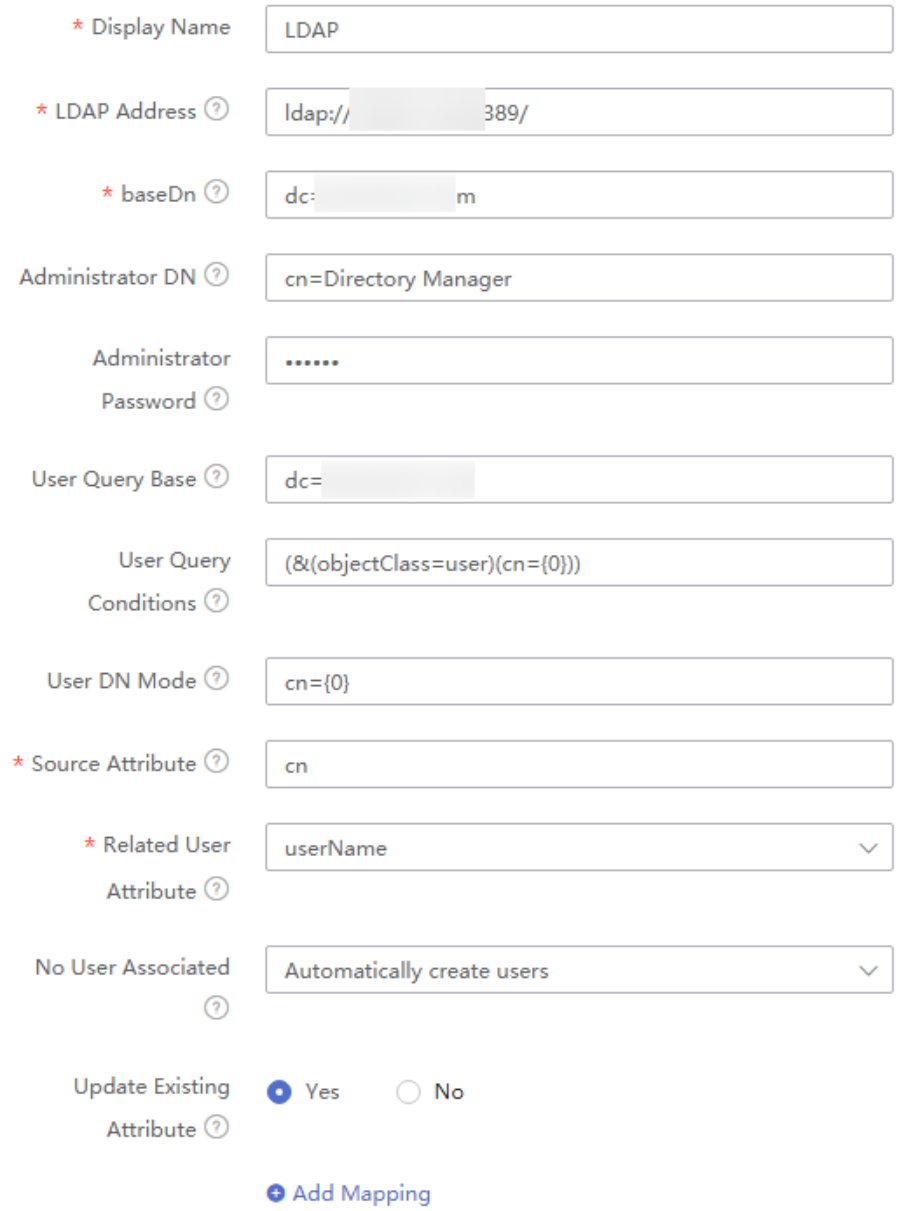


Table 4-12 Configuration parameters

Parameter	Mandatory	Description
Display Name	Yes	Display name of the authentication provider, for example, **LDAP**.
LDAP Address	Yes	Connection address of LDAP in the format "ldap://*{hostname}*:*{port}*/", where *{hostname}* indicates the LDAP server address and *{port}* indicates the port number. The default port is 389. For details, see **Setting Up an LDAP Server**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
baseDn	Yes	Root node of the LDAP directory used to authenticate users. The format of the value is "dc=,dc=". For details, see **Setting Up an LDAP Server**.
Administrator DN	No	Identifier of the administrator. The default value is **cn=Directory Manager**.
Administrator Password	No	Password of the LDAP administrator.
User Query Base	No	Base DN of users. The default value is **ou=People**.
User Query Conditions	No	Filter conditions for matching system users in LDAP. The default value is **(&(objectClass=user)(uid={0}))**. For details, see **LDAP Filters**. Condition-based search has lower priority than DN-based query.
User DN Mode	No	Search path of LDAP users. The default value is **uid={0},ou=people**. DN authentication takes precedence over other authentication modes.
Source Attribute	Yes	LDAP username attribute. The default value is **uid**. You can obtain the attribute in **Step 3**.
Related User Attribute	Yes	User attribute mapped by LDAP in the system. The user attribute must be a unique text.
No User Associated	Yes	Operation that will be performed if a user logs in successfully but fails to be associated with a system user.

To map other attributes, such as username, set **No User Associated** to **Automatically create users**, and add the desired mappings. For details, see **Table 4-13**.

Table 4-13 Mapping parameters

Parameter	Description
User Attribute	Attribute in OneAccess that maps to LDAP.
Mapping Type	Mode of user attribute mapping between OneAccess and LDAP.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication Provider Attribute Name	Name of the corresponding user attribute in LDAP.

----End

Enabling LDAP Authentication

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Resources** > **Applications**. Then select **UserCenter** in the **Pre-integrated Applications** section.

Step 3 On the application information page, click the application icon.

Step 4 On the application details page, choose **Login Settings** > **Web Applications**, enable LDAP authentication, and select the authentication provider added in **Adding an LDAP Authentication Provider**.

CAUTION

The password text box will be used during LDAP authentication. To enable LDAP authentication, disable database authentication and AD authentication first.

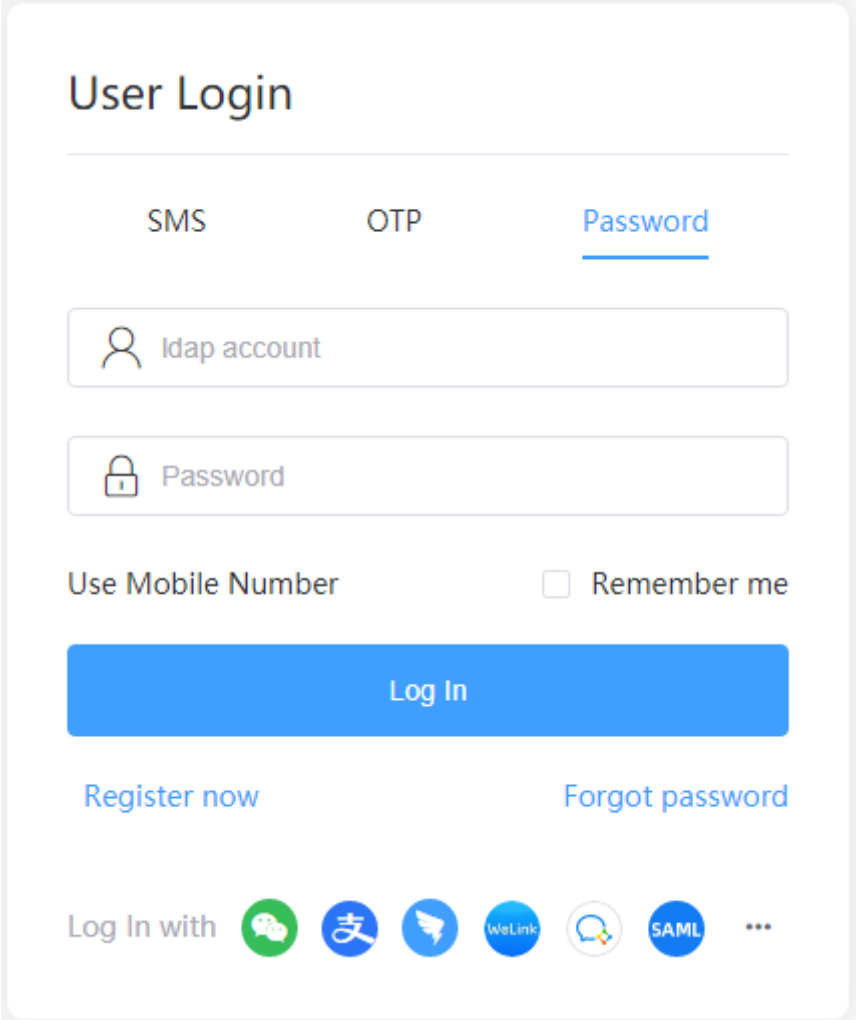
----End

Logging In to the User Portal Through LDAP Authentication

- Go to the user portal login page, select **Password**, enter an LDAP account and password, and click **Log In**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-48 Selecting Password



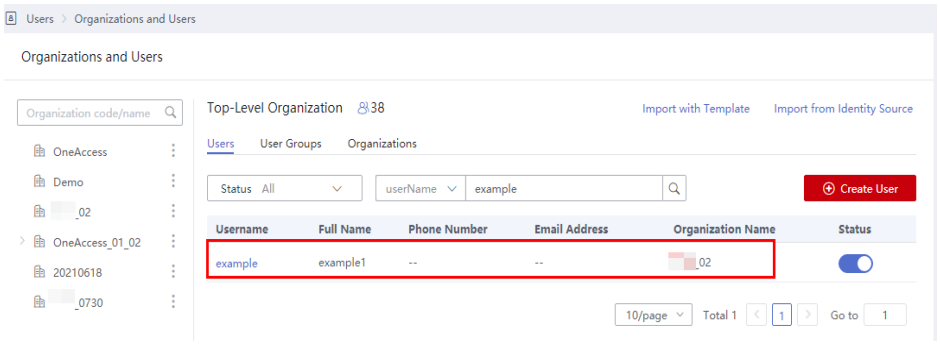
- After login, go to the administrator portal, choose **Users** > **Organizations and Users**, and view the automatically created user.

  NOTE

  - To automatically create a new user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 4-12**.
  - By default, users automatically created in the preceding scenario belong to the first root organization in the administrator portal.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-49 Viewing users



4.7 Kerberos Authentication

Kerberos is a computer-network authentication protocol that allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. For details, visit **https://web.mit.edu/kerberos**.

AD is a database that stores network objects, allowing administrators and users to search for required information.

Service Principal Name (SPN) is a unique identifier of a service instance.

It associates a service instance with a service account during Kerberos authentication. SPNs must be registered for the server under a built-in computer account or user account. For built-in accounts, SPNs are automatically registered. To run services using a domain account, manually register an SPN for the account.

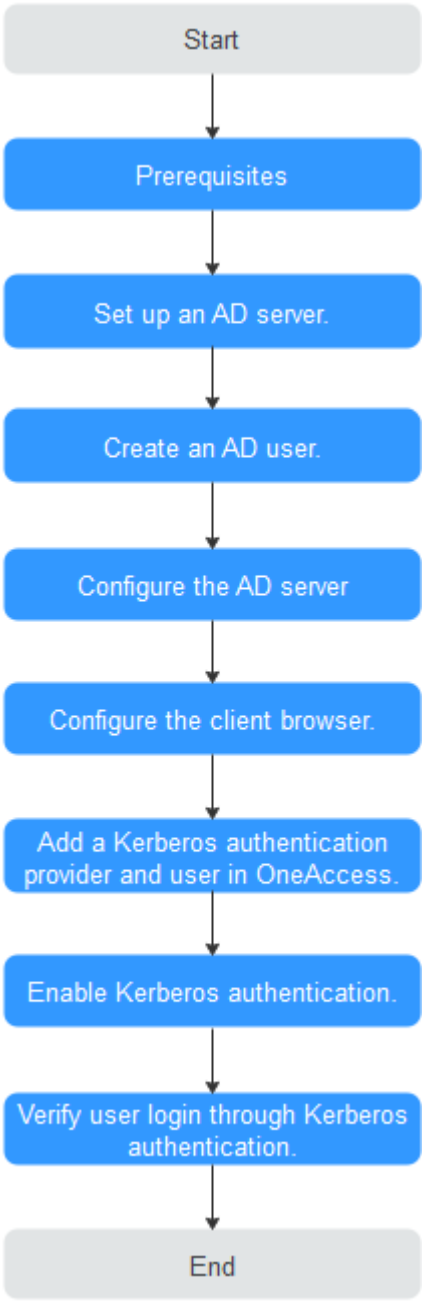
This section describes how to integrate Kerberos with OneAccess.

NOTE

The procedure for accessing the user portal on a PC is used for illustration. Select and configure an application that meets your service requirements.

 Copyright © Huawei Technologies Co., Ltd.

Configuration process



Setting Up an AD Server

Windows Server 2012 R2 is used as an example to describe how to set up a domain server. For details, see **Setting Up an AD Server**.

Creating an AD User

Create an AD user in the established AD domain.

Step 1 Go to the AD management center.

Step 2 Right-click the target domain, choose **New** > **User**, enter the user information, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

To prevent login exceptions, configure the user with unlimited password validity.

----End

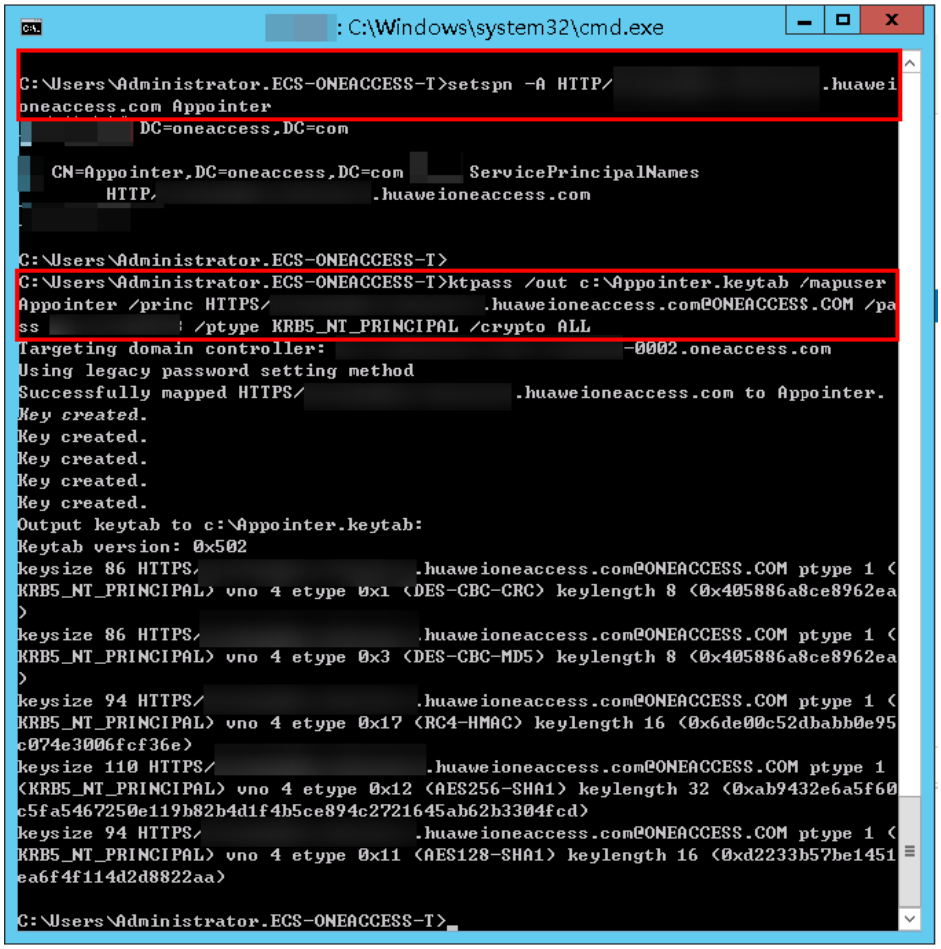
Configuring the AD server

Step 1 Generate an SPN in the AD server.

In the DOS window of the AD server, run the "**setspn -A HTTP/***{Tenant domain name} {AD username}*" command, for example, **setspn -A HTTP/xxxxxx.huaweioneaccess.com Appointer**.

Step 2 Generate a keytab file in the AD server.

In the DOS window of the AD server, run the "**ktpass /out** *{Keytab file path}* **/mapuser** *{AD username}* **/princ HTTPS/***{Tenant domain name}*@*{AD domain name}* **/pass** *{AD user password}* **/ptype KRB5_NT_PRINCIPAL /crypto All**" command, for example, **ktpass /out c:\Appointer.keytab /mapuser Appointer /princ HTTPS/xxxxxx.huaweioneaccess.com@ONEACCESS.COM /pass {AD user password} /ptype KRB5_NT_PRINCIPAL /crypto All**.



Step 3 Configure an appointment in the AD server.

- Select the user created in **Creating an AD User**, right-click **Properties**, and configure an appointment.

 Copyright © Huawei Technologies Co., Ltd.

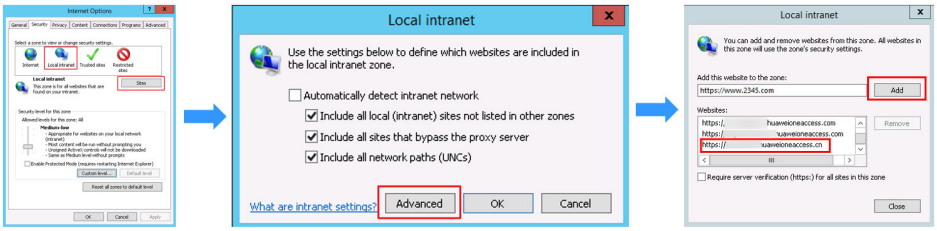
- If you choose to only trust this user for appointing a service, add the service you want to appoint.

----End

Configuring the Client Browser

- Internet Explorer

  Open Internet Explorer, choose **Tools** > **Internet options** > **Security** > **Local intranet** > **Sites** > **Advanced**, and add the website **https://***{Tenant domain name}*.



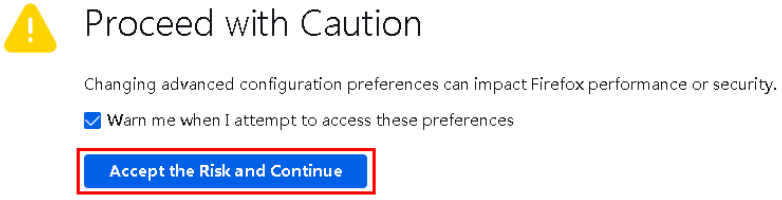
- Google Chrome

  Google Chrome shares the configurations of Internet Explorer. After configuring Internet Explorer, directly use Google Chrome without additional configurations.

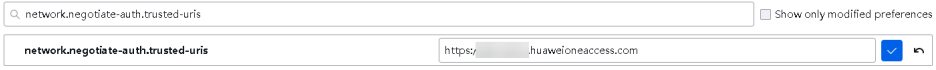
- Mozilla Firefox

  a. Open the Firefox browser, enter **about:config** in the address box, and click **Accept the Risk and Continue**.





  b. Enter **network.negotiate-auth-trusted-uris** and set the value to **https://***{Tenant domain name}*.



Adding a Kerberos Authentication Provider

Step 1 Log in to the administrator portal.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 In the top navigation pane, choose **Authentication** > **Authentication Providers**, and click **Kerberos**. On the **Kerberos Authentication Providers** page, click **Add Authentication Provider** in the upper right and set the parameters.

Figure 4-50 Adding an authentication provider

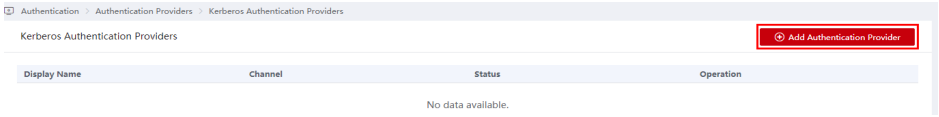


Figure 4-51 Configuring parameters

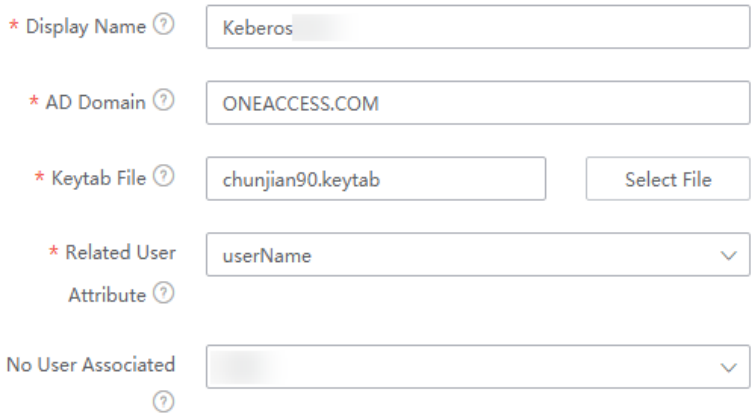
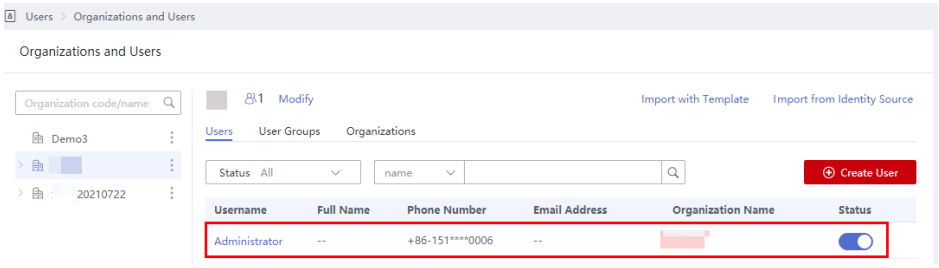


Table 4-14 Configuration parameters

Parameter	Description
* Display Name	Display name of the authentication provider, for example, **Kerberos**.
* AD Domain	AD domain name in upper case, for example, **ONEACCESS.COM**.
* Keytab File	Select the file generated in **Step 2**.
* Related User Attribute	Unique attribute, for example, user ID, to associate with a system user.
No User Associated	Indicates that the login fails if no user is associated during authentication.

Step 3 In the top navigation pane, choose **Users** > **Organizations and Users**. Select the target organization, click **Create User**, and enter the user information. Ensure that the username is the same as that of the AD domain account.

 Copyright © Huawei Technologies Co., Ltd.



----End

Enabling Kerberos Authentication

Step 1 Log in to the administrator portal.

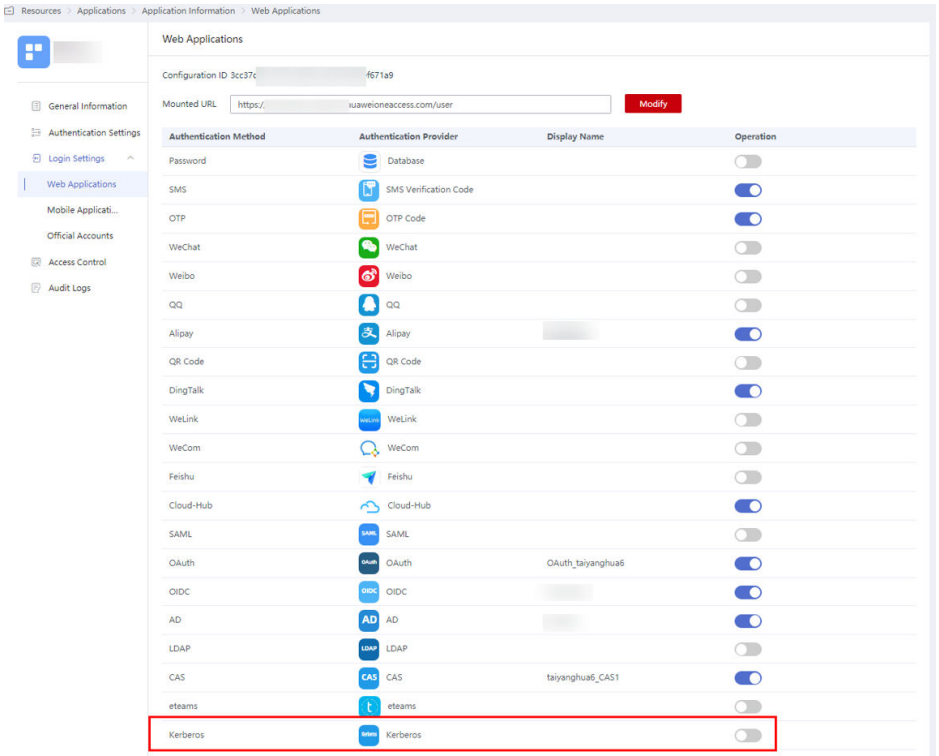
Step 2 In the top navigation pane, choose **Resources** > **Applications**. Then select **UserCenter** in the **Pre-integrated Applications** section.

Step 3 On the application information page, click the application icon.

Step 4 On the application details page, choose **Login Settings** > **Web Applications**, enable Kerberos authentication, and select the authentication provider added in **Adding a Kerberos Authentication Provider**.

NOTE

Once enabled, Kerberos authentication is preferentially used when users access the user portal. To use other authentication modes, disable Kerberos authentication first.



----End

 Copyright © Huawei Technologies Co., Ltd.

Logging In to the User Portal Through Kerberos Authentication

Step 1 Log in to the AD domain.

Step 2 Access the user portal as the user who logs in to the AD domain in **Step 1**, using Google Chrome, Internet Explorer, or Firefox in password-free mode.

----End

4.8 eteams Authentication

OneAccess supports user identity authentication through eteams. After you integrate an eteams authentication provider with OneAccess, common users can log in to different applications by scanning QR codes with eteams.

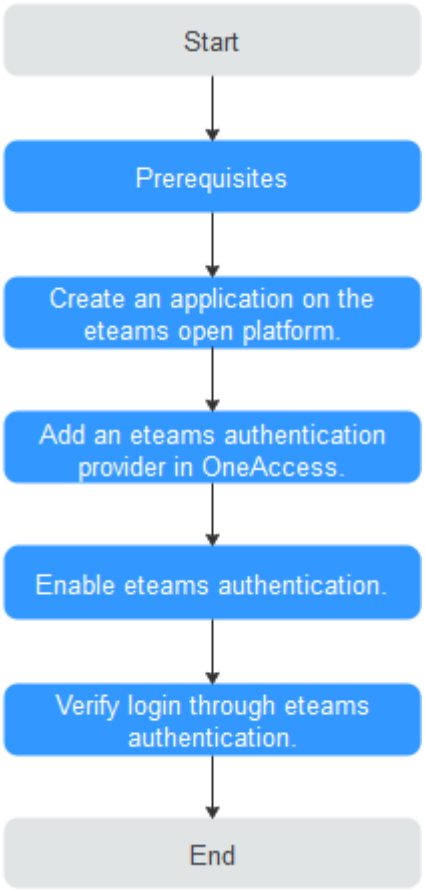
This section describes how to integrate eteams with OneAccess.

NOTE

The procedure for accessing the user portal on a PC is used for illustration. Select and configure an application that meets your service requirements.

Configuration Process

Figure 4-52 Configuration process



 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- You have a developer account for the eteams open platform.
- You have permissions to access the administrator portal.

Creating an Application on the eteams Open Platform

Create an application and configure authorization information for OneAccess on the eteams open platform to establish a trust on OneAccess.

Step 1 Log in to the eteams open platform at **https://open.eteams.cn/appinfo/list#**.

Step 2 Create an application for logging to third-party applications from eteams in password-free mode, and click **Next**. Then set the application information.

Step 3 Submit the information for review. After the application is approved, obtain the app_key.

----End

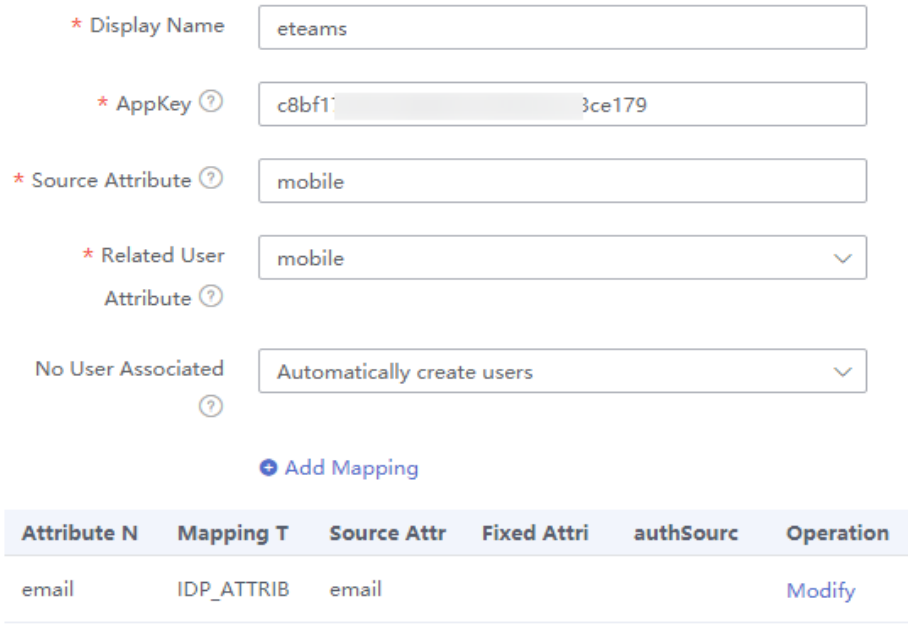
Adding an eteams Authentication Provider

Add an eteams authentication provider and configure the application information in OneAccess.

Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Authentication** > **Authentication Providers**, and click **eteams**. On the **eteams Authentication Providers** page, click **Add Authentication Provider** in the upper right and set the parameters.

Figure 4-53 Configuring parameters



 Copyright © Huawei Technologies Co., Ltd.

Table 4-15 Configuration parameters

Parameter	Description
* Display Name	Name of the authentication provider.
* AppKey	app_key of an application created and approved on the eteams open platform. For details, see **Step 3**.
* Source Attribute	The attribute returned upon successful eteams authentication. It is associated with OneAccess users. Options: **mobile** and **email**.
* Related User Attribute	User attribute in OneAccess to be associated with eteams.
No User Associated	Authentication logic used when no OneAccess users are associated.

To map other attributes, such as email, set **No User Associated** to **Automatically create users**, and add the desired mappings. For details, see **Table 4-16**.

Table 4-16 Mapping parameters

Parameter	Description
User Attribute	User attribute in OneAccess to be associated with eteams.
Mapping Type	Mode of user attribute mapping between OneAccess and eteams.
Authentication Provider Attribute Name	Name of the corresponding user attribute in eteams.

----End

Enabling eteams Authentication

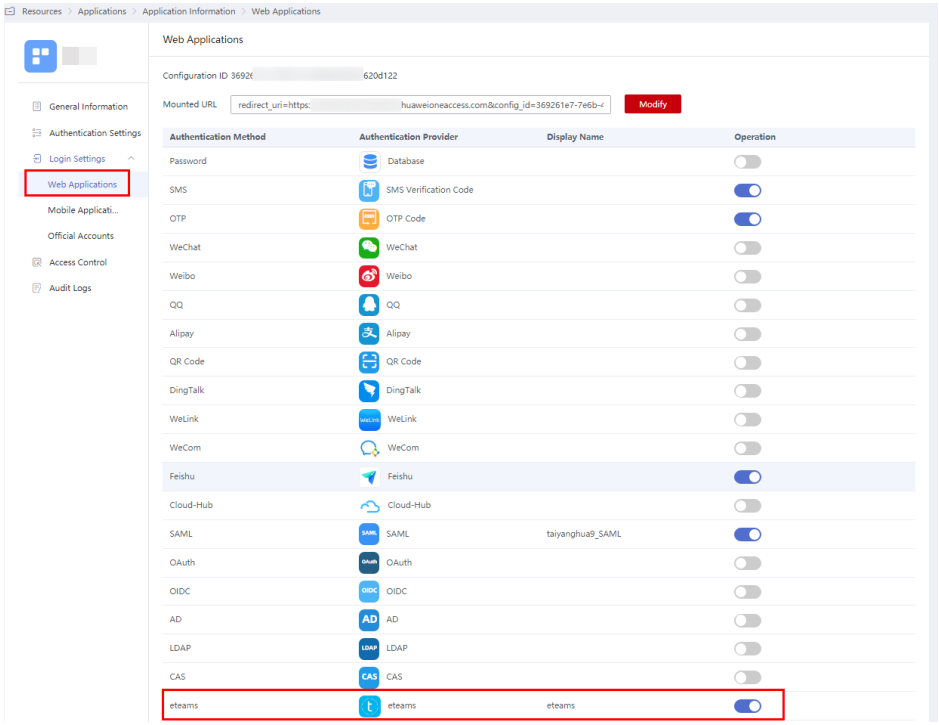
Step 1 Log in to the administrator portal.

Step 2 In the top navigation pane, choose **Resources** > **Applications**. Then select **UserCenter** in the **Pre-integrated Applications** section.

Step 3 On the application information page, click the application icon.

Step 4 On the application details page, choose **Login Settings** > **Web Applications**, enable eteams authentication, and select the authentication provider you added.

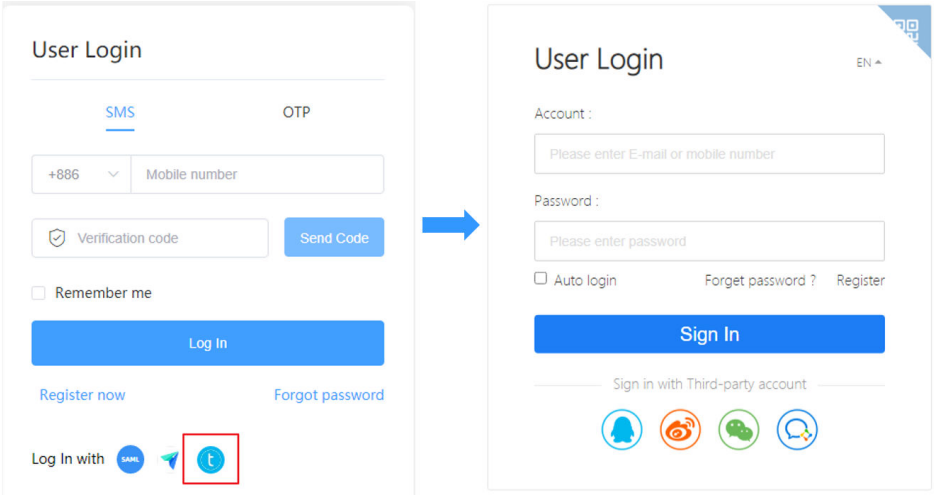
 Copyright © Huawei Technologies Co., Ltd.



----End

Logging In to the User Portal Through eteams Authentication

- Go to the user portal login page, select **eteams**, enter an eteams account and password, and click **Log In**. Alternatively, switch to the QR code login page and scan the QR code using your eteams client.

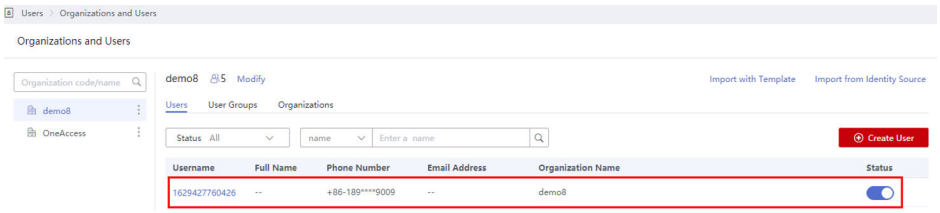


- After login, go to the administrator portal, choose **Users** > **Organizations and Users**, and view the automatically created user.

  NOTE

  - To automatically create a new user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 4-15**.
  - By default, users automatically created in the preceding scenario belong to the first root organization in OneAccess.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

5 Interconnection with HUAWEI CLOUD

SSO Access to HUAWEI CLOUD

5.1 SSO Access to HUAWEI CLOUD

Introduction

HUAWEI CLOUD provides the identity provider function to implement federated identity authentication based on SAML or OIDC. This function allows users in your enterprise to access resources in your HUAWEI CLOUD account through SSO using their IdP accounts.

Basic Concepts

- IdP

  An IdP collects and stores user identity information (such as usernames and passwords), and authenticates users when they log in. When users use their IdP accounts to log in to HUAWEI CLOUD through SSO, the IdP is OneAccess.

- SP

  An SP uses the user information provided by trusted IdP to provide services for users. When users use their IdP accounts to log in to HUAWEI CLOUD through SSO, the SP is HUAWEI CLOUD.

- SSO

  SSO is an access type that allows users to access a trusted SP system after logging in to the enterprise IdP. For example, after a trust relationship is established between OneAccess and HUAWEI CLOUD, users in OneAccess can use their existing accounts and passwords to access HUAWEI CLOUD through the login link in OneAccess.

- SAML 2.0

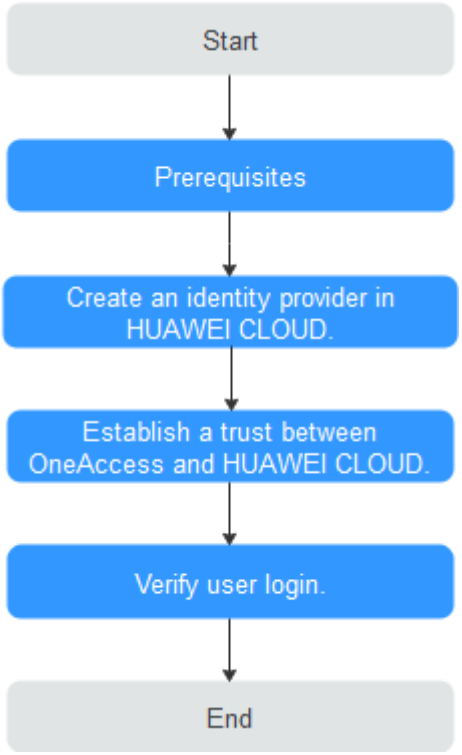
  SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about an end user between an IdP and SP. It is an open standard ratified by the OASIS and is being used by many IdPs. For more information about this standard, see **SAML 2.0 Technical Overview**.

This document describes the implementation and configuration of SSO access from OneAccess to HUAWEI CLOUD through SAML.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process

Figure 5-1 Configuration process



Prerequisites

- You have permissions to access the administrator portal.
- You have a HUAWEI CLOUD account. To register one, see **Registering with HUAWEI CLOUD and Completing Real-Name Authentication**.

Creating an Identity Provider on HUAWEI CLOUD

Create an identity provider and configure the metadata file on the HUAWEI CLOUD console.

Step 1 Download the metadata file of OneAccess.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Settings** > **Server Settings**. Then click **IdP**.
3. On the **IdP** page, click **Download IdP Metadata** in the upper right. The metadata file is automatically saved.

Step 2 Create an identity provider on HUAWEI CLOUD. For details, see **Creating an Identity Provider on HUAWEI CLOUD**.

Step 3 Configure the metadata file on HUAWEI CLOUD. For details, see **Configuring the Metadata File for the Enterprise Identity Provider**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Configure the metadata file of OneAccess obtained in **Step 1**.
- To view, modify, or delete the identity provider, see **Viewing, Modifying, and Deleting an Identity Provider**.

----End

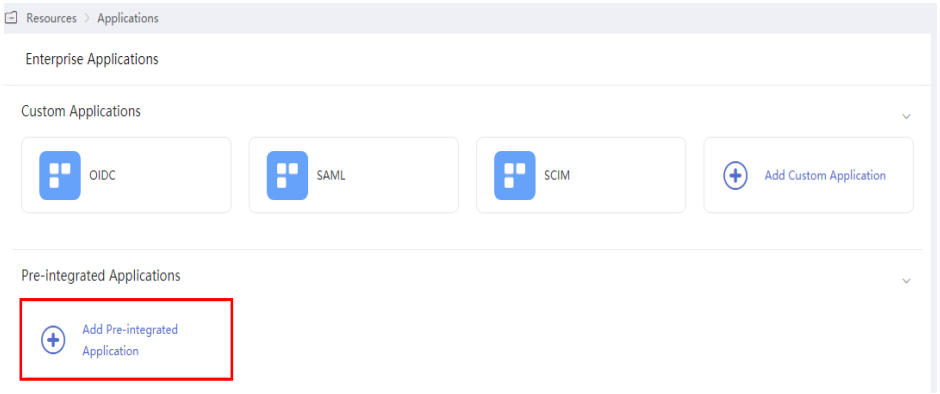
Establishing a Trust Between OneAccess and HUAWEI CLOUD

Configure the metadata file of HUAWEI CLOUD in OneAccess to establish a trust on HUAWEI CLOUD.

Step 1 Add the HUAWEI CLOUD application in OneAccess.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Resources** > **Applications**.
3. Click **Add Pre-integrated Application** in the **Pre-integrated Applications** section.

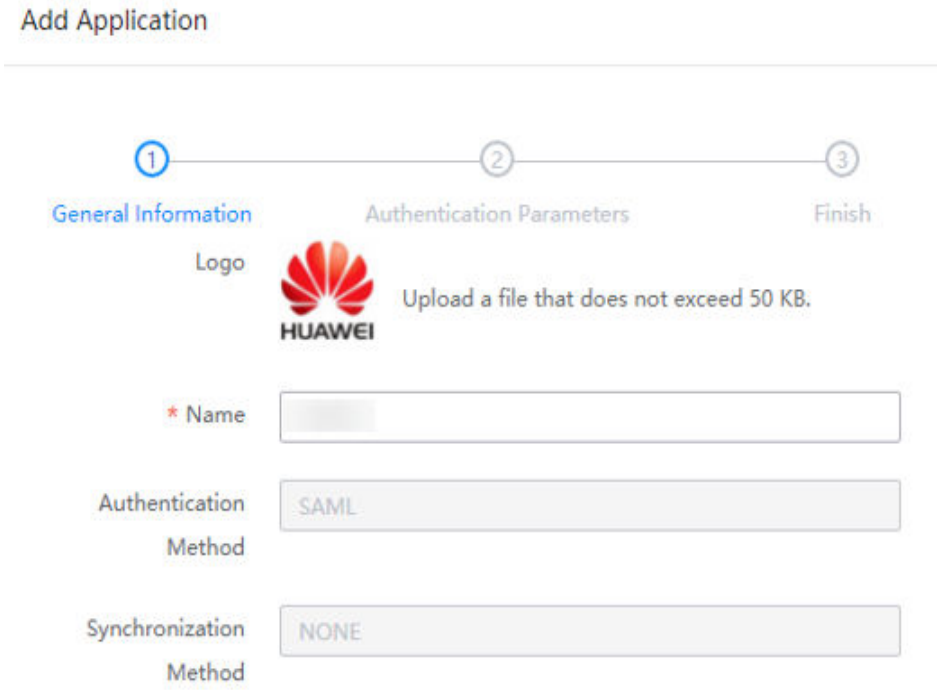
Figure 5-2 Adding a pre-integrated application



4. On the **Add Pre-integrated Application** page, click **HUAWEI CLOUD**.
5. On the **Add Application** page, confirm the general information, and click **Next**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-3 Confirming general information

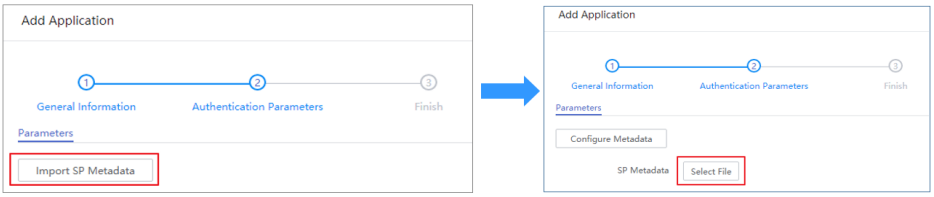


6. On the **Authentication Parameters** page, choose **Import SP Metadata**, click **Select File**, select the HUAWEI CLOUD metadata file, and click **Open**. The system automatically extracts the metadata.

   NOTE

   - To obtain the metadata file of HUAWEI CLOUD, visit **https://auth.huaweicloud.com/authui/saml/metadata.xml**, and save the metadata as **SP-metadata.xml**.
   - Alternatively, manually configure the metadata. For details, see **Editing metadata**.

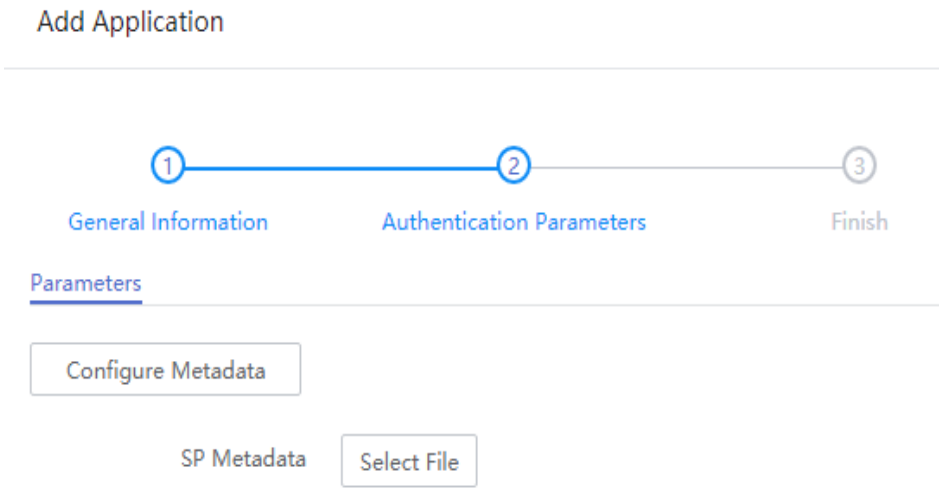
Figure 5-4 Uploading a metadata file



7. When the **Select File** button changes to √, the system has extracted the metadata. Click **Next**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-5 Metadata extracted



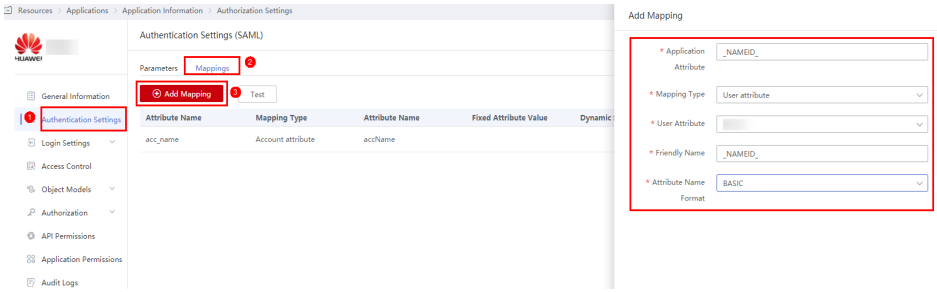
Step 2 Configure mappings between OneAccess and HUAWEI CLOUD.

NOTE

For details about how to configure login, access control, and object models, see **Modifying Application Configurations**.

1. Click the HUAWEI CLOUD application added in **Step 1**. On the application information page, click the **HUAWEI CLOUD** icon to go to the application details page.
2. Choose **Authentication Settings** > **Mappings**, and click **Add Mapping** to configure mappings. For details about the parameters, see **Mappings**.

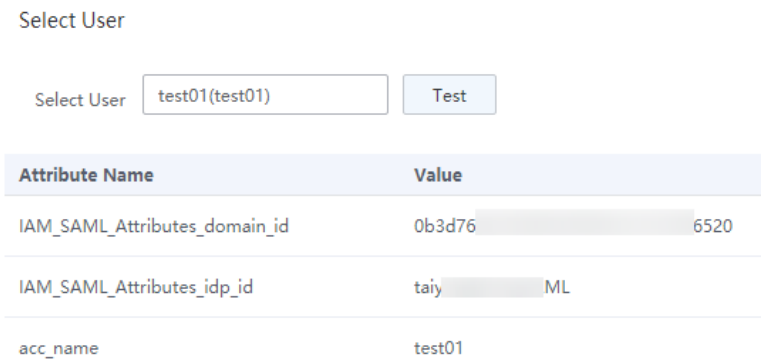
Figure 5-6 Adding a mapping



3. Click **Test**. On the **Select User** page, enter a username to test the mappings.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-7 Testing mappings



Step 3 Configure the login link in OneAccess.

Choose **Login Settings** > **Web Applications**, click **Modify**, and replace the URL with the login link of the identity provider created in **Step 2**.

NOTE

For details about how to obtain the login link of the identity provider, see **Logging In as a Federated User**.

Step 4 Authorize users to access HUAWEI CLOUD.

1. In the left pane, choose **Authorization** > **Application Accounts**. Then click **Add Accounts**, select users, and click **Save**. To authorize access using a policy, see the descriptions about the application account authorization policy in **Modifying Application Configurations**.

Figure 5-8 Adding accounts

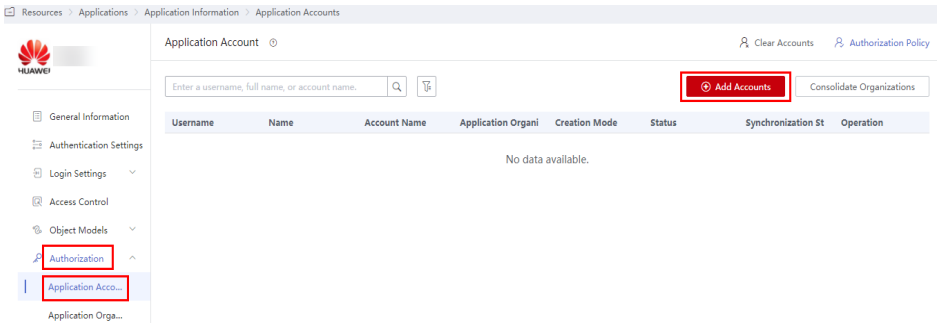
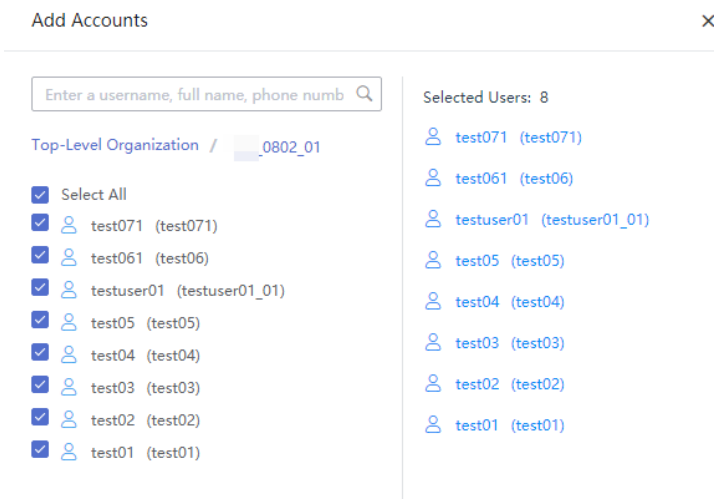


Figure 5-9 Selecting users



----End

Logging In as a User

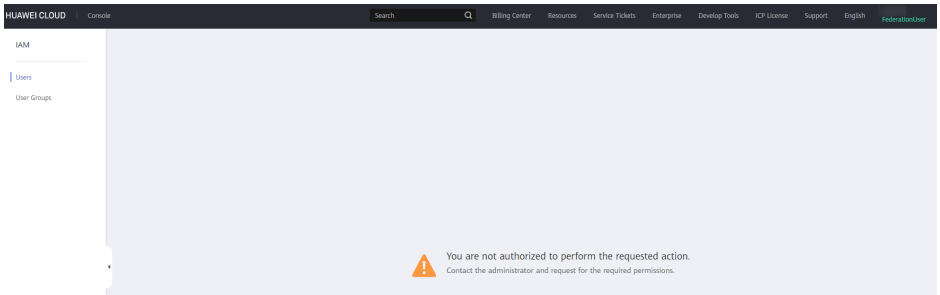
Log in to the user portal as one of the users authorized in **Step 4**, and click **HUAWEI CLOUD** to access it.

- The following message is displayed if no identity conversion rules are configured for the identity provider in **Step 2**.

  NOTE

  The OneAccess user only has read permissions for HUAWEI CLOUD by default.

  Figure 5-10 No permissions

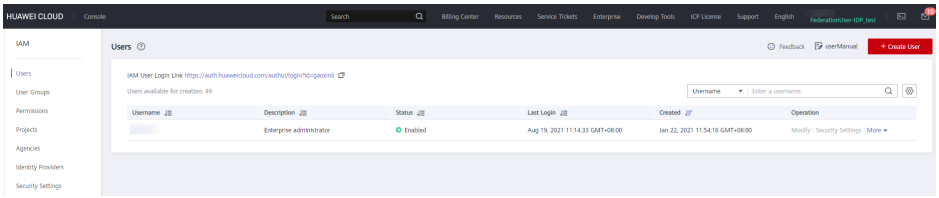
- The following page is displayed if identity conversion rules are configured for the identity provider in **Step 2**.

  NOTE

  - The OneAccess user has admin permissions.
  - To assign permissions to OneAccess users, configure identity conversion rules for the identity provider. For more information, see **Configure Identity Conversion Rules**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-11 admin permissions granted



 Copyright © Huawei Technologies Co., Ltd.

6 Authorizing IAM Users to Access a OneAccess Instance

Identity and Access Management (IAM) provides permissions management for secure access to your HUAWEI CLOUD services and resources. IAM is free of charge.

You can use your account to create IAM users and assign permissions for specific resources. Each IAM user has their own identity credentials (password and access keys) and uses cloud resources based on assigned permissions.

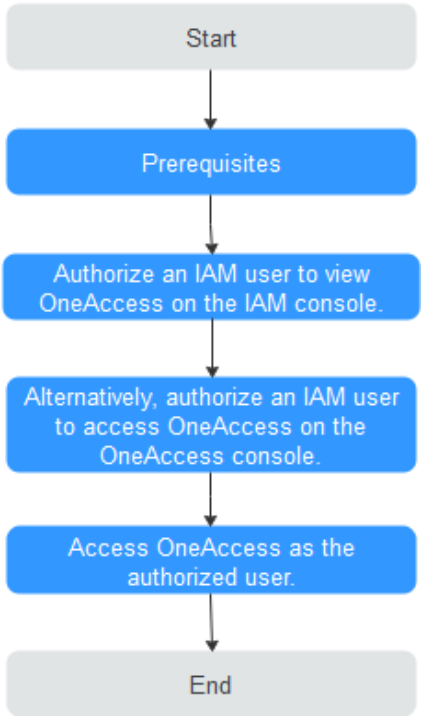
To log in to HUAWEI CLOUD from OneAccess through SSO, see **SSO Access to HUAWEI CLOUD**.

IAM users can access OneAccess instances, helping the enterprise administrator to securely control access to OneAccess resources.

This section describes how to authorize IAM users to access a OneAccess instance.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process



Prerequisites

You have a HUAWEI CLOUD account and have used the account to purchase a OneAccess instance. For details about how to purchase an instance, see **Buying an Instance**.

Authorizing IAM Users to View OneAccess

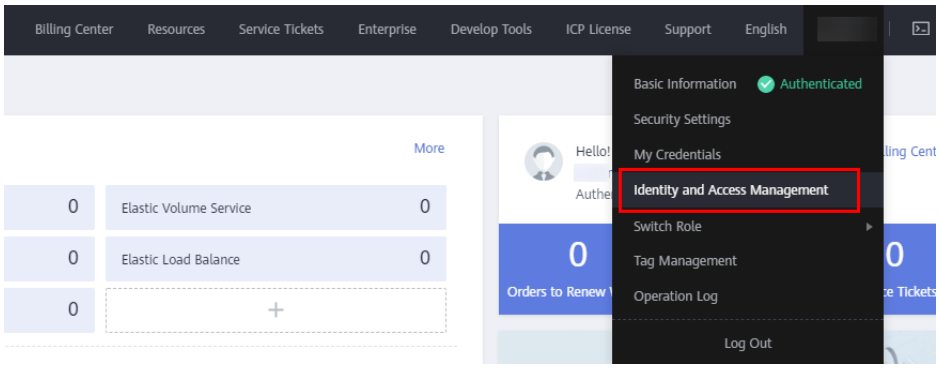
Create users and add them to user groups that have the required permissions in IAM. The users then inherit permissions of these groups.

Step 1 Log in to HUAWEI CLOUD and click **Console** in the upper right. For details, see **Logging In to HUAWEI CLOUD**.

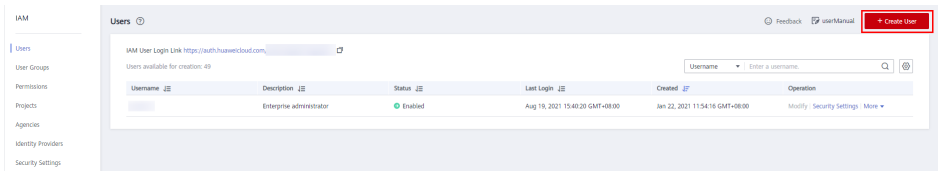


Step 2 On the management console, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.

Copyright © Huawei Technologies Co., Ltd.

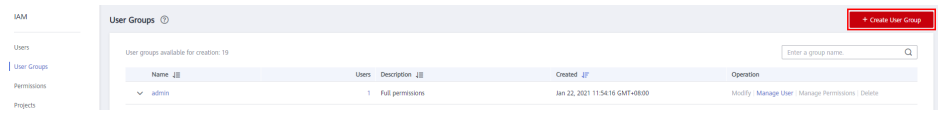


Step 3 In the navigation pane of the IAM console, choose **Users**. Then click **Create User**, enter the user information, set the access type, and click **Next**.



Step 4 Click **Create**. For details, see **Creating an IAM User**.

Step 5 In the navigation pane, choose **User Groups**. Then click **Create User Group**, enter a user group name, and click **OK**. For details, see **Creating a User Group**.



Step 6 In the user group list, click **Manage Permissions** in the **Operation** column of the row that contains the user group created in **Step 5**. On the **Permissions** tab page, click **Assign Permissions**.

Figure 6-1 Manage Permissions

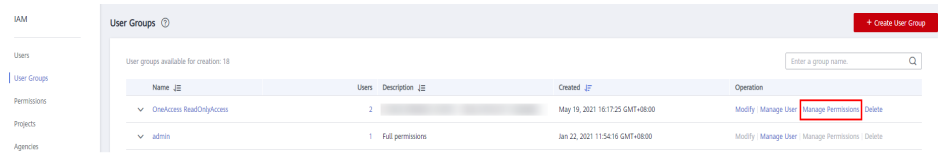
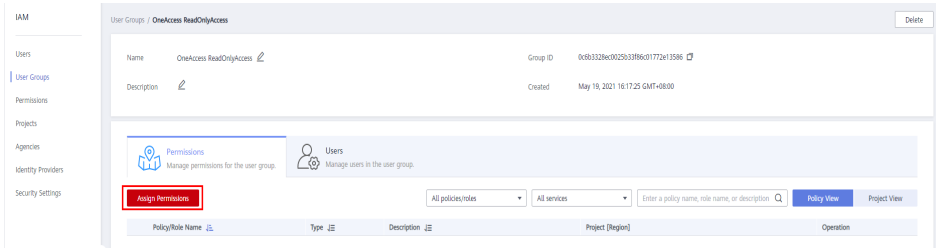


Figure 6-2 Assign Permissions

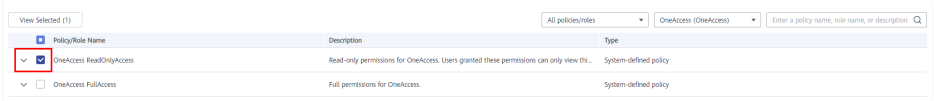


Step 7 Select **OneAccess ReadOnlyAccess** and click **OK**. For details, see **Assigning Permissions to a User Group**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

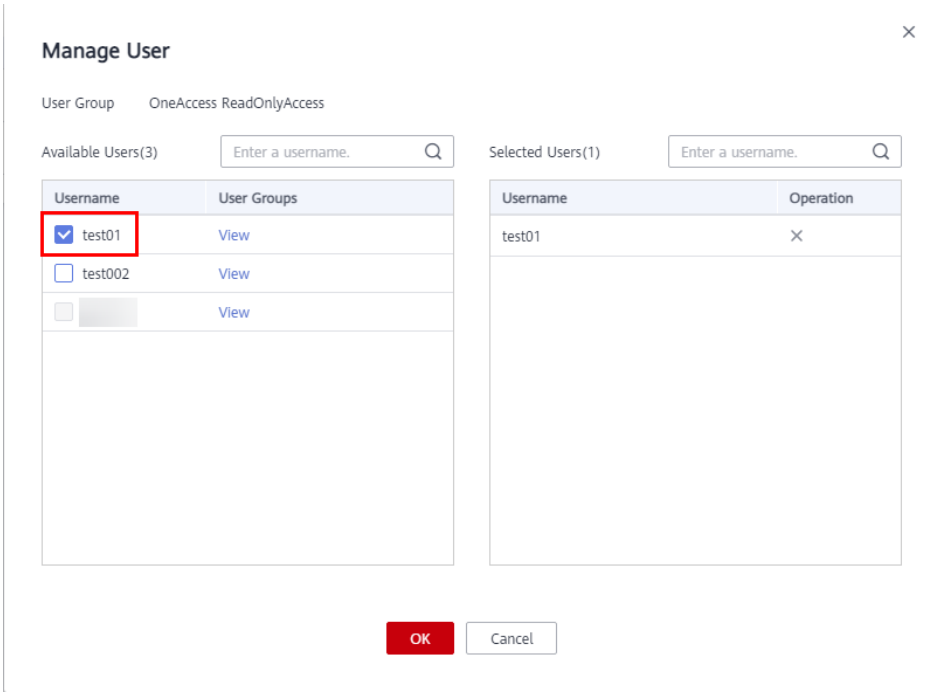
To assign the user group all permissions for OneAccess, select **OneAccess FullAccess**.



Step 8 In the user group list, click **Manage User** in the row that contains the group authorized in **Step 7**.



Step 9 Select the user created in **Step 4** and click **OK**. To remove a user from the user group, see **Removing Users from a User Group**. Now, you have completed authorization of the IAM user.



----End

Authorizing IAM Users to Access OneAccess

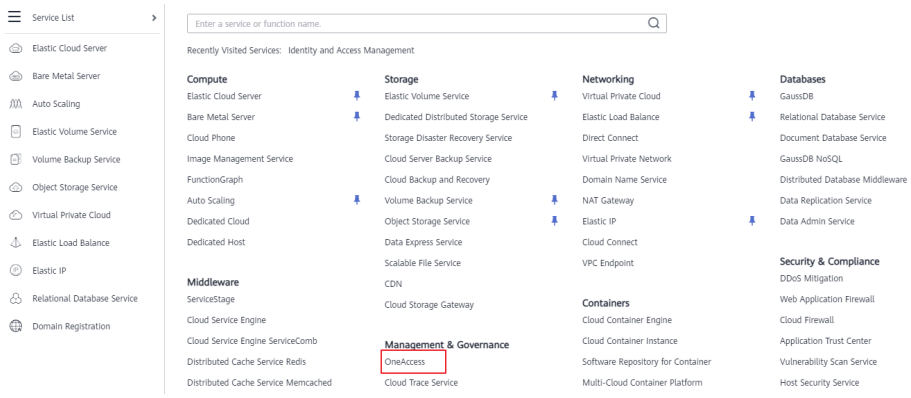
Authorize IAM users to access OneAccess in the OneAccess console.

Step 1 Log in to HUAWEI CLOUD and click **Console** in the upper right. For details, see **Logging In to HUAWEI CLOUD**.

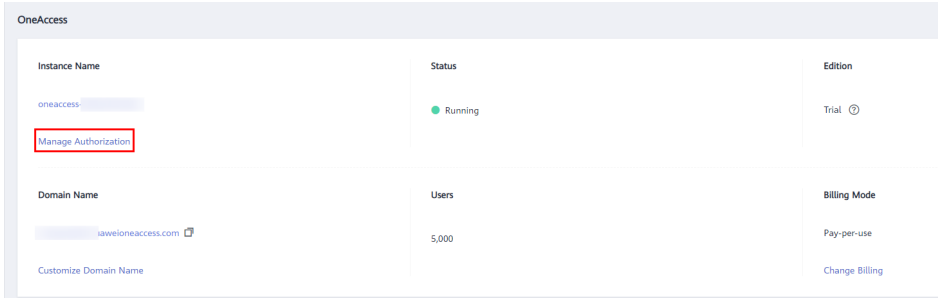


 Copyright © Huawei Technologies Co., Ltd.

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



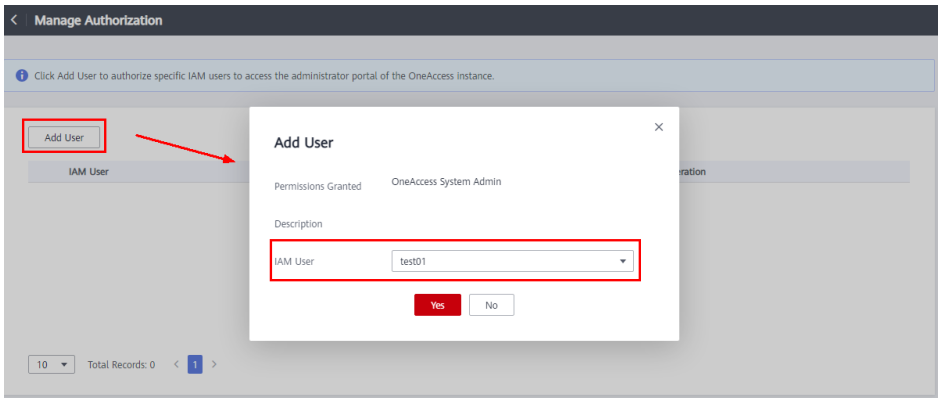
Step 3 Click **Manage Authorization**.



Step 4 Click **Add User** and select the user mentioned in **Step 9**.

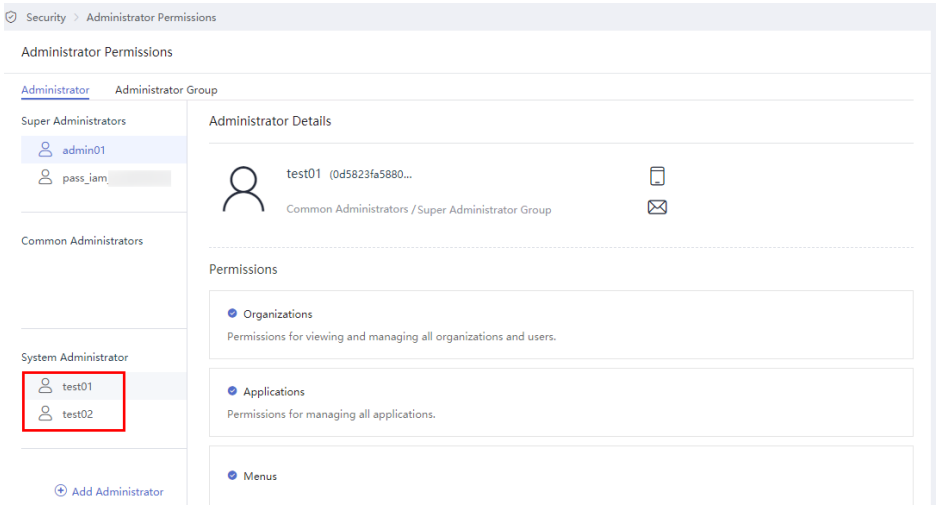
NOTE

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



Step 5 Go to the administrator portal, and view the system administrator that is automatically generated.

 Copyright © Huawei Technologies Co., Ltd.



----End

Accessing OneAccess as an Authorized IAM User

Log in to HUAWEI CLOUD and access the OneAccess administrator portal.

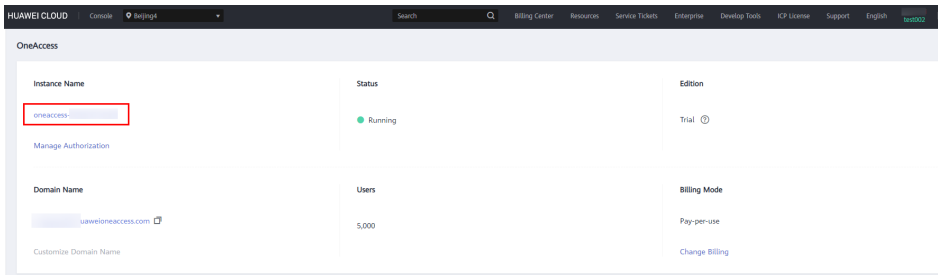
Step 1 Log in to HUAWEI CLOUD as the IAM user. For details, see **Logging In as an IAM User**.

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.

NOTE

- By default, IAM users do not have permissions for the **Administrator Permissions** page. For details about other operations, see **Enterprise Administrator Guide**.
- To grant the IAM user all permissions for OneAccess, select the **OneAccess FullAccess** policy. For details, see **Step 7**.



----End

 Copyright © Huawei Technologies Co., Ltd.

7 Voice Gateway Configuration

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

- Built-in gateway

  For details, see **Built-in Gateway**.

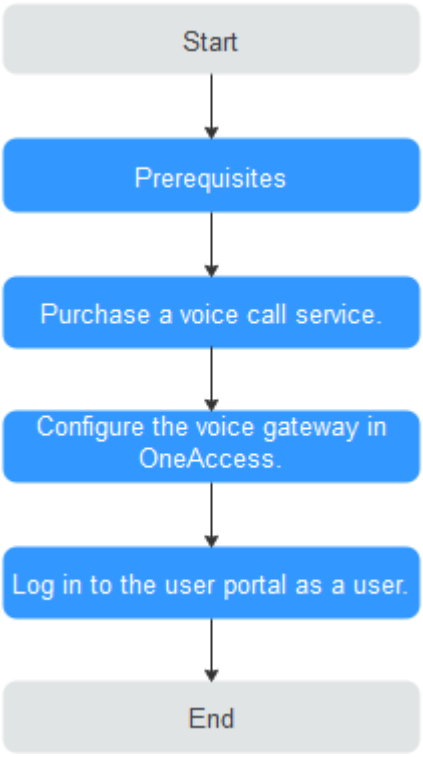
- Custom gateway

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

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

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process



Prerequisites

You have permissions to access the administrator portal.

Buying a Voice Call Service

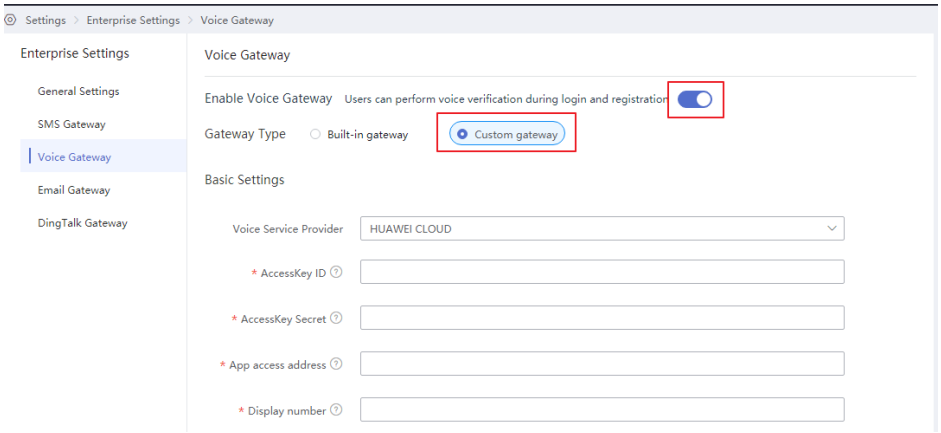
If you have already purchased a service, skip this step.

Configuring Voice Gateway in OneAccess

Step 1 Log in to the administrator portal.

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

Step 3 On the **Enterprise Settings** page, choose **Voice Gateway**, enable the voice gateway function, select **Custom gateway**, and set the basic parameters.



 Copyright © Huawei Technologies Co., Ltd.

Table 7-1 Basic settings

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

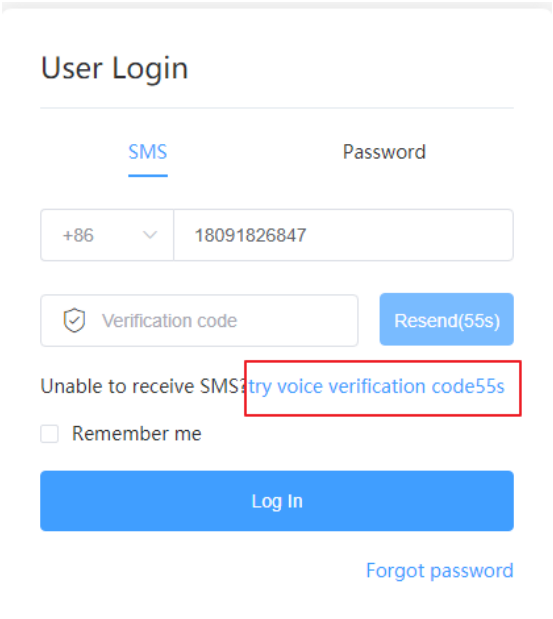
Step 4 Configure the template IDs and codes and click **Save**.

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

----End

Logging In to the User Portal

Go to the user portal, select **SMS**, click **try voice verification code**, and enter the received voice verification code to log in to the user portal.



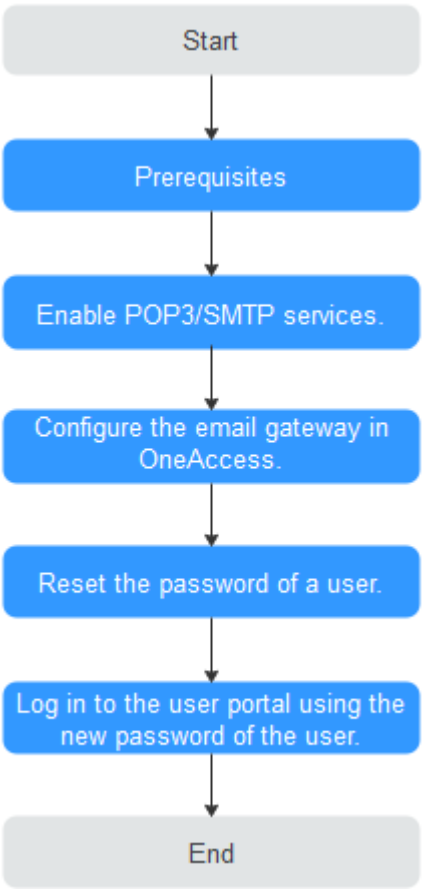
 Copyright © Huawei Technologies Co., Ltd.

8 Email Gateway Configuration

The email gateway helps users obtain information through emails during password resetting. If you enable the email gateway, OneAccess generates random passwords during password resetting and send them to users by email. The users can then use the received passwords to log in and reset their passwords.

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

Configuration Process



 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- You have an email account.
- You have permissions to access the administrator portal.

Enabling POP3/SMTP Service

Go to the email account management page, enable POP3/SMTP service by following on-screen instructions, and save the authorization code.

NOTE

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

Configuring Email Gateway in OneAccess

Step 1 Log in to the administrator portal.

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

Step 3 On the **Enterprise Settings** page, choose **Email Gateway**, enable the email gateway, and set the basic parameters.

Figure 8-1 Configuring the email gateway

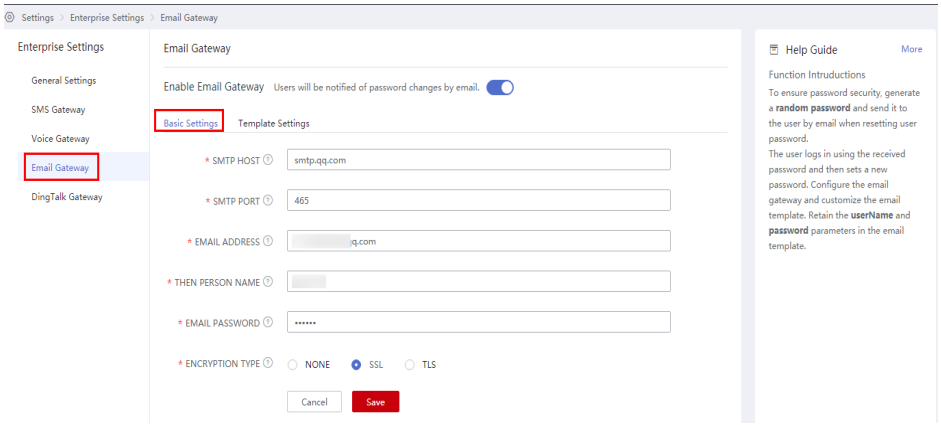


Table 8-1 Basic settings

Parameter	Mandatory	Description
SMTP HOST	Yes	Address of the host that provides SMTP services. Obtain the value of this parameter in the documentation of the email gateway service platform.
SMTP PORT	Yes	Port for providing SMTP services. The default port is 465.
EMAIL ADDRESS	Yes	Email address of your enterprise, that is, the address from which system emails will be sent.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
THEN PERSON NAME	Yes	Name of the email sender.
EMAIL PASSWORD	Yes	Authorization code obtained in **Enabling POP3/SMTP Service**.
ENCRYPTION TYPE	Yes	Email encryption mode, which must be the same as that specified on the email gateway service platform. Obtain the value of this parameter in the documentation of the email gateway service platform.

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

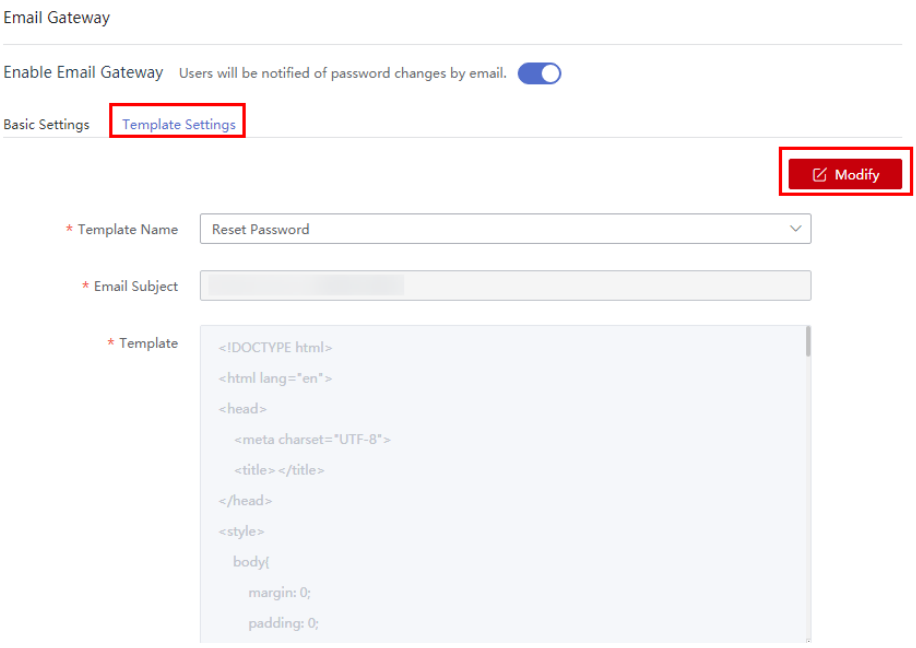


Table 8-2 Template settings

Parameter	Mandatory	Description
Template Name	Yes	The default template name is "Reset Password".
Email Subject	Yes	The default subject is **Reset Password**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Description
Template	Yes	This parameter is customizable.

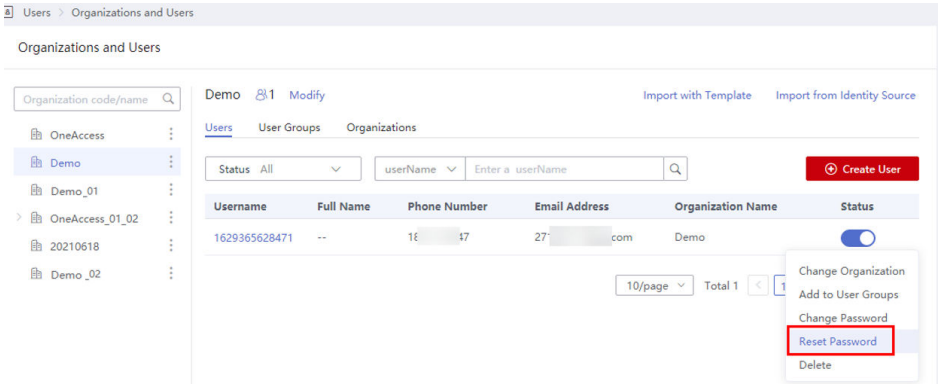
----End

Resetting User Password

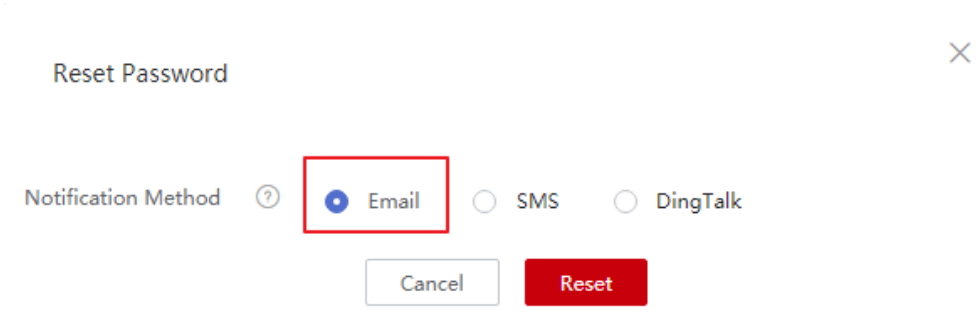
Step 1 Log in to the administrator portal.

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

Step 3 Choose **More** > **Reset Password** in the row that contains the target user.



Step 4 In the **Reset Password** dialog box, select **Email** and click **Reset**. A message is displayed indicating that the email is sent.

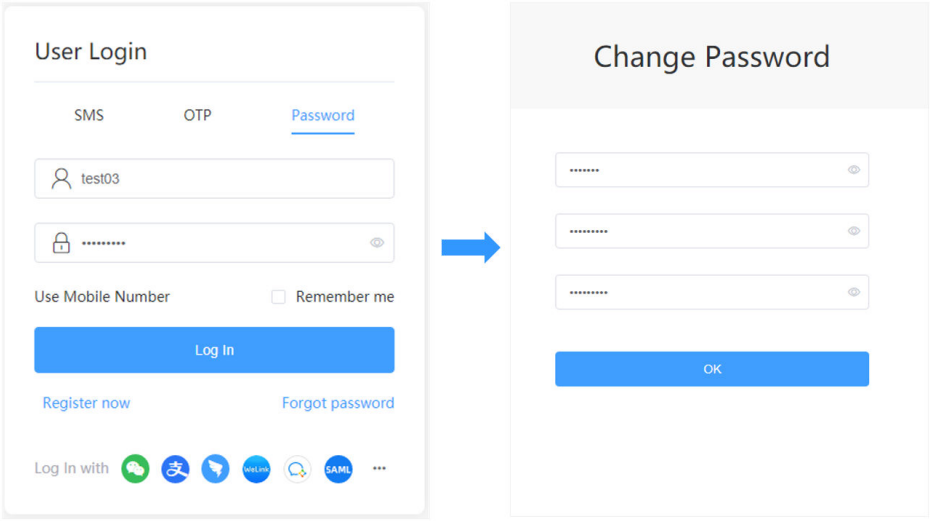


----End

Logging In to the User Portal

Log in to the user portal using the username and password provided in the email, and then change the password.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.