OneAccess

Best Practices

Issue	01
Date	2025-06-11

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 OneAccess Best Practices

This section summarizes best practices of OneAccess in common scenarios. Each practice is given a description and procedure.

Table 1-1 Best practices for identity source integration

Practice	Description
Integrating AD	OneAccess allows you to import user and organization information from AD and synchronize the information in real time via LDAPv3.
Integrating LDAP	OneAccess allows you to import user and organization information from LDAP and synchronize the information in real time via LDAPv3.

Table 1-2 Best practices for application integration

Practice	Description
Logging In to the Huawei Cloud Through User Portal	Huawei Cloud supports single sign-on (SSO) based on SAML and OpenID Connect. After enterprise administrators configure Huawei Cloud and OneAccess, common users can log in to the OneAccess user portal to access the Huawei Cloud console or a specific Huawei Cloud application without entering a password.

Practice	Description
SSO Access to Applications Through SAML	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.
SSO Access to Applications Through OAuth 2.0	OAuth 2.0 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.
SSO Access to Applications Through OIDC	OpenID Connect (OIDC) is a standard identity authentication protocol that runs on top of the OAuth 2.0 protocol. For more information about OpenID Connect, see **OpenID Connect Introduction**. This section describes how to integrate an application with OneAccess using the OIDC protocol.
SSO Access to Applications Through CAS	CAS is an HTTP2- and HTTP3-based protocol which requires that each component 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.
SSO Access to Applications Through Plug-in Autocompletion	OneAccess can integrate applications that do not support standard protocols (including OAuth 2.0, SAML, OpenID Connect, and CAS) and cannot be reconstructed on a PC. This section describes how to integrate an application with OneAccess through plug-in autocompletion.

Table 1-3 Best practices for data synchronization

Practice	Description
Synchronizing Data to Atlassian Through SCIM	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. This section describes how to synchronize user data to Atlassian through the SCIM protocol.
Synchronizing Data Through LDAP	LDAP is a 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 internal networks of their company after logging in on a PC for once.

Table 1-4 Best practices for authentication provider integration

Practice	Description
Built-in Authentication Providers	This practice describes how to add a FIDO2 authentication provider (such as facial or fingerprint biometric authentication) to log in to applications on OneAccess.
SAML Authentication	OneAccess allows you to configure the SAML protocol as the authentication provider to log in to each application system for better user experience.

Practice	Description
OIDC Authentication	OneAccess allows you to configure the OIDC protocol as the authentication provider to log in to each system for better login modes and experience. OpenID Connect (OIDC) is a standard identity authentication protocol that runs on top of the OAuth 2.0 protocol. For more information about OpenID Connect, see **OpenID Connect Introduction**.
CAS Authentication	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. OneAccess allows you to configure the CAS protocol as the authentication provider. You can use the CAS protocol to log in to each application system and implement single sign-on (SSO) between application systems.

Practice	Description
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. OneAccess allows you to configure the OAuth protocol as the authentication provider. You can use the OAuth protocol to log in to each application system.
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. OneAccess allows you to configure the Kerberos protocol as the authentication provider. You can use the Kerberos protocol to log in to each application system.

Practice	Description
AD Authentication	Active Directory (AD) is a database that stores network objects, allowing administrators and users to search for required information. To facilitate user authentication, OneAccess uses LDAP to direct the authentication to the AD domain. After the AD authentication succeeds, OneAccess matches the user attributes returned by the AD domain with the user association attributes in OneAccess. If the authentication is successful, the user can log in to OneAccess.
LDAP Authentication	Lightweight Directory Access Protocol (LDAP) is a 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 internal networks of their company after logging in on a PC for once.

Table 1-5 Other best practices

Practice	Description
Authorizing IAM Users to Access a OneAccess Instance Administrator Portal	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. IAM users can access OneAccess instances, helping the enterprise administrator to securely control access to OneAccess resources.

Practice	Description
API Usage	OneAccess provides a third-party API authorization management function. API providers configure APIs in OneAccess first. To use these APIs, API consumers obtain authentication tokens from OneAccess, and call the APIs with the authentication tokens. The API providers then determine whether to provide services to the API consumers based on the authentication tokens.
Configuring MFA for User Login	OneAccess supports MFA during user login, which is more secure. This section uses the user portal as an example to describe how to configure and use MFA.

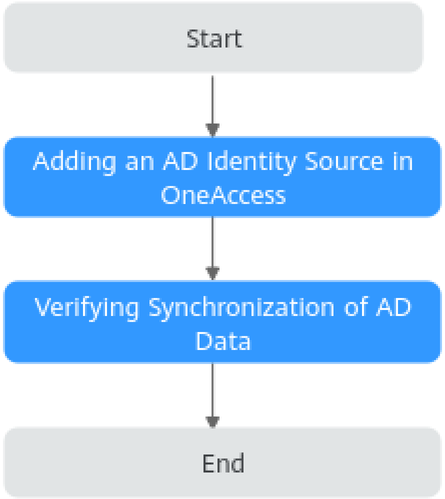
2 Identity Source Integration

2.1 Integrating AD

Active Directory (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. OneAccess allows you to import user and organization information from AD and synchronize the information in real time via LDAPv3.

This section describes how to integrate AD with OneAccess.

Configuration Process


Start
Adding an AD Identity Source in OneAccess
Verifying Synchronization of AD Data
End

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

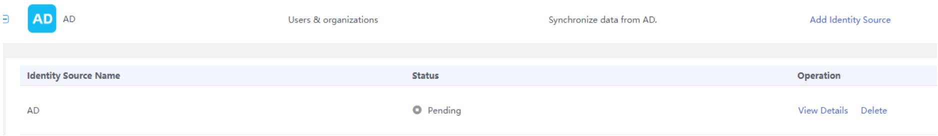
Configure parameters of the AD identity source so that OneAccess can synchronize data from it.

Step 1 Add an identity source in OneAccess.

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

Step 2 Configure the import settings.

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



AD AD Users & organizations Synchronize data from AD. Add Identity Source

Identity Source Name	Status	Operation
AD	Pending	View Details Delete

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

Table 2-1 Basic settings

Parameter	Description
* Host	Host name or IP address of the AD server.
*TCP Port	TCP/IP port of the AD server. The default port is **389**. OneAccess can be accessed only over public networks. Provide the public network address of your server and enable port **389**.
SSL	Default value: **true**, which indicates that SSL is used to connect the AD server.
StartTLS	Whether to enable startTLS for encrypted communication. ▪ **true**: StartTLS is enabled, and SSL cannot be set to **true**. ▪ **false**: Disable StartTLS.
Certificate Verification	Whether to verify the certificate. This parameter is valid only when SSL or StartTLS is set to **true**. **true**: Verify the certificate. **false**: Do not verify the certificate. The certificate must be authenticated by the public network. Self-signed certificates cannot be used.

Parameter	Description
Protocol Version	Default value: **TLSv1.2**. Recommended: **TLSv1.3** and **TLSv1.2**.
Principal	Identifier used for AD server authentication. Specify an account that has read permission for the AD domain. The input parameter will contain the domain name, for example, **admin@test.com** and **TEST\admin**.
*Password	Password of the principal account.
* Base Contexts	One or more root nodes (for example, **OU=huaweitest,DC=test,DC=com**) in the AD tree to be considered as the beginning for synchronizing AD users.
*UID Attribute	Name of the AD attribute mapped to the UID attribute.
* Account Object Class	One or more object classes to be used when a new user object is created in the AD tree. If you enter multiple object classes, each item occupies a line. Do not use commas (,) or semicolons (;) to separate multiple object classes. Some object classes may require you to specify all object classes in the class hierarchy.

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

Table 2-2 Optional settings

Parameter	Description
Domain	If a domain name exists, it should be excluded from the reclaimed username. If there are multiple domain names, separate them with commas (,). The default username excludes the domain name.
Account Username Attribute	Saves one or more attributes of an account username. During authentication, these attributes are used to search for the AD entry of the username to be authenticated.

Parameter	Description
Organization Object Class	One or more object classes that will be used when a new organization object is created in the AD tree. If you enter multiple object classes, each item occupies a line. Do not use commas (,) or semicolons (;) to separate multiple object classes. Some object classes may require you to specify all object classes in the class hierarchy.
Organization Name Attribute	Stores one or more attributes of the organization name. During authentication, these attributes are used to search for the AD entry of the organization name to be authenticated.
Failover Servers	Lists all servers that will be used for failover when the preferred server fails. If the preferred server fails, JNDI will connect to the next available server in the list. Lists all servers in the "**ldap://ldap.example.com:389/**" format (compliant with the standard AD v3 URL described in RFC 2255). Only the host and port parts of the URL are relevant in this setting.
Password Attribute	Name of the AD attribute used to store passwords. When the password of a user is changed, a new password will be set for this attribute.
AD Filter	Optional AD filter used to control the accounts returned from AD resources. If no filter is specified, only accounts containing all specified object classes are returned.

Parameter	Description
Password Hash Algorithm	Algorithm used by the identity system to hash passwords. Currently, **SSHA**, **SHA**, **SMD5**, and **MD5** are supported. A null value indicates that the system does not hash the password. Unless the LDAP server performs hashing (Netscape Directory Server and iPlanet Directory Server perform hashing), this will result in plaintext passwords being stored in AD.
Preferentially process the change of the resource password policy after reset	If this resource is specified in the login module (i.e., this resource is the passing verification target) and the password policy of the resource is configured to change after reset, users who have reset the resource account password for management purpose need to change the password after successful verification.
Use VLV Controls	Specifies whether to forcibly use the VLV control on the standard AD control. The default value is **false**.
VLV Sort Attribute	Sorting attribute used for VLV indexes on resources.
Read Schema	If the value is **TRUE**, the connector reads the schema from the server. If **FALSE**, the connector provides a default schema based on the object class in the configuration. To use the extended object class, this attribute must be set to **TRUE**.
Basic Contexts to Synchronize	One or more starting points in the AD tree that are used to determine whether changes should be synchronized. If this attribute is not set, the base context attribute is used to synchronize changes.

Parameter	Description
Object Class to Synchronize	Object class to be synchronized. The change log is for all objects; it filters updates based on the listed object classes. You should not list the superclasses of an object class unless you want to synchronize the object with any superclass value. For example, if only the "inetOrgPerson" object should be synchronized, but the superclasses ("person", "organizationalperson", and "top") of "inetOrgPerson" should be filtered out, only "inetOrgPerson" should be listed here. All objects in AD are derived subclasses of "top". Therefore, "top" should never be listed. Otherwise, no object can be filtered.
Attribute to Synchronize	Name of the attribute to be synchronized. When this option is set, if updates in the change log do not update any named attributes, these updates are ignored. For example, if only "department" is listed, only changes that affect "department" are processed and all other updates are ignored. If you leave it blank (default setting), all changes are processed.
AD Filter for Accounts to Synchronize	Optional AD filter used during object synchronization. Because the change log applies to all objects, this filter updates only the objects that meet the specified filter criteria. If a filter is specified, the object is synchronized only when the object meets the filter conditions and contains the synchronized object class.
Change Log Block Size	Number of change log entries obtained by each query.
Change Number Attribute	Change the number attribute.

Parameter	Description
Filter with Or Instead of And	Typically, the filter used to obtain change log entries is to retrieve change entries over a period of time based on the AND condition. If this attribute is set, the OR condition will be used as the filter for the required number of changes.
Remove Log Entry Object Class from Filter	If this attribute is set (default), the filter used to obtain change log entries will not contain the "changeLogEntry" object class because the change log should not contain entries of other object classes.
Password Attribute to Synchronize	Name of the password attribute to be synchronized.
Status Management Class	Used to manage the enabling/ disabling status. If no class is specified, identity status management cannot be performed.
Whether to search for passwords	Indicates whether to retrieve the user password during search. Default value: **No**.
DN attribute	DN attribute name of an item. The default value is **entryDN**.
AD Filter	An optional AD filter that controls the groups returned from AD resources. If no filter is specified, only groups containing all specified object classes are returned.
Read Timeout (ms)	Time for waiting for a response. If no response is received within the specified time, the read attempt is aborted. If the value is 0 or less than 0, there is no limit.
Connection Timeout (ms)	Waiting time for opening a new server connection. The value 0 indicates that the TCP network timeout will be used, which may be several minutes. If the value is less than 0, there is no limit.

Parameter	Description
Account DN Prefix	The default value is **cn**. You can also set it to another attribute name used as the DN prefix, such as uid.

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

Table 2-3 Advanced settings

Parameter	Description
Enable timer for recycling	You can set whether to enable scheduled reclamation. If scheduled reclamation is enabled, the reclamation task is executed at a specified time every day.
Timer frequency	Fixed: one day **NOTE** Displayed when scheduled reclamation is enabled.
Select a recycling start time	You can set the reclamation start time in the drop-down list box. **NOTE** This parameter needs to be set only when scheduled reclamation is enabled.
Organization	Parent organization in OneAccess to which organizations will be synchronized from AD. A new top-level organization will be automatically created if this parameter is not set.
Organization Matching	Mapping between the enterprise AD and OneAccess organizations. This policy is used when OneAccess synchronizes organizations from the enterprise AD. For example, OneAccess has an organization attribute **Code** and your AD has a similar attribute **Organization Code**. Organizations in your AD will be mapped to OneAccess, and their codes in the AD will be identified as organization codes in OneAccess.
Create Organization	Enabled by default, indicating that OneAccess will automatically create organizations that do not match any organizations in OneAccess. To ensure data integrity, enable this option.
Update Organization	Enabled by default, indicating that organizations in OneAccess that match those synchronized from the identity source will be updated. To ensure data accuracy, keep this option enabled.

Parameter	Description
Delete Organization	After organization data is synchronized from the AD to OneAccess, if you want to delete organizations from the AD, OneAccess compares the number of deleted organizations with the configured deletion threshold. If the ratio of the number of deleted organizations to the total number of data records synchronized last time is greater than the threshold, the deletion fails; if the ratio of the number of deleted organizations to the total number of data records synchronized last time is less than the threshold, the deletion is successful.
User Matching	Mapping between an AD user and a OneAccess user. Used when OneAccess synchronizes users from the enterprise AD. For example, OneAccess has a user attribute **User ID** and your AD has a similar attribute **Employee ID**. Users in your AD will be mapped to OneAccess, and their employee IDs in the AD will be identified as user IDs in OneAccess.
Create User	Enabled by default, indicating that OneAccess will automatically create users who do not match any users in OneAccess. To ensure data integrity, enable this option.
Update User	Enabled by default, indicating that users in OneAccess that match those synchronized from the identity source will be updated. To ensure data accuracy, keep this option enabled.
Delete User	After AD user data is successfully synchronized to OneAccess, if you want to delete a user from AD, OneAccess compares the number of deleted users with the configured deletion threshold. If the ratio of the number of deleted users to the total number of users synchronized last time is greater than the threshold, the deletion fails; if the ratio of the number of deleted users to the total number of data records synchronized last time is less than the threshold, the deletion is successful.
Disable User Threshold Adjustment	The default value is 20%. This is a customizable protection mechanism provided by the platform. When the number of data records disabled or deleted by the upstream identity source application exceeds the threshold, the platform will not disable or delete the data synchronously after receiving the instruction.

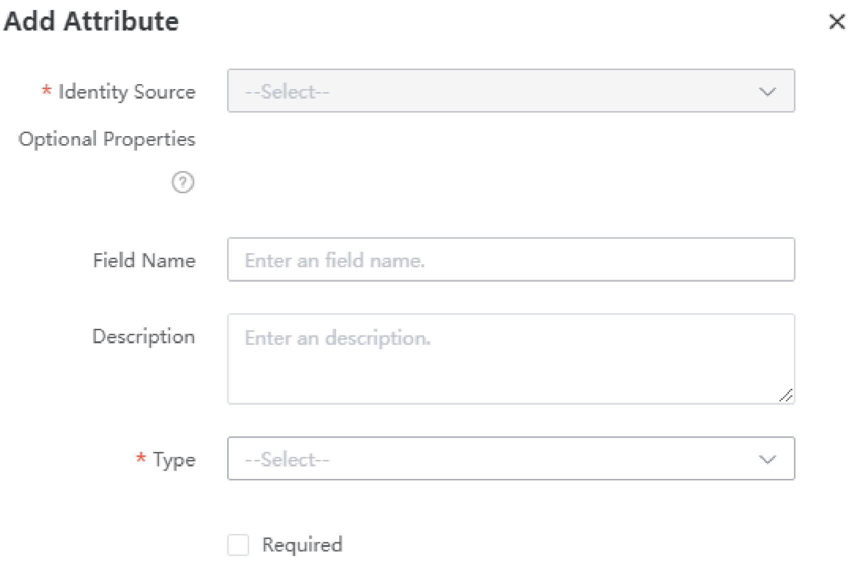
Step 3 (Optional) Set the object models.

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

Table 2-4 Object model

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

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



Add Attribute

* Identity Source: --Select--

Optional Properties

Field Name: Enter an field name.

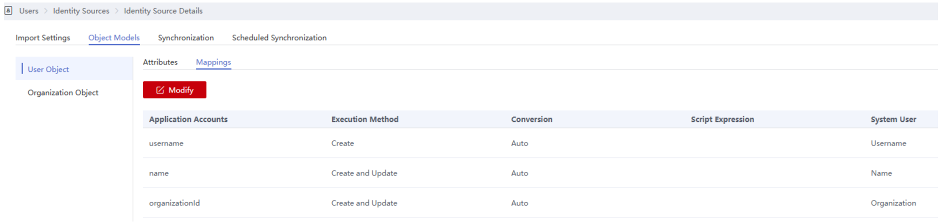
Description: Enter an description.

* Type: --Select--

□ Required

  b. Select the optional attributes of the identity source, and enter the display tag and description.
  c. Select a type. When **Type** is set to **Text**, you need to set **Format**.
  d. Set whether the attribute is mandatory and click **OK**. The attribute is added.
- Set the mapping rule.

  On the **Mapping Definition** tab page, click **Modify**. Set the conversion mode, script expression mode, execution mode, and system user for the mapping rule.



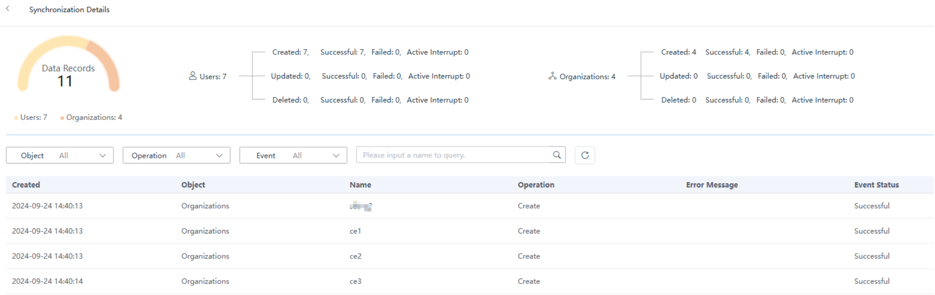
Application Accounts	Execution Method	Conversion	Script Expression	System User
username	Create	Auto		Username
name	Create and Update	Auto		Name
organizationId	Create and Update	Auto		Organization

----End

Verifying Synchronization of AD Data

- Synchronization via import
  a. In the AD identity source list, click **View Details** in the row that contains the target identity source. Click the **Synchronization** tab, and click **Execute**. OneAccess synchronizes user and organization data from the AD identity source, and generates operation records.
  b. Click **View Details** in the row that contains the target record to view details.

Figure 2-1 Viewing details



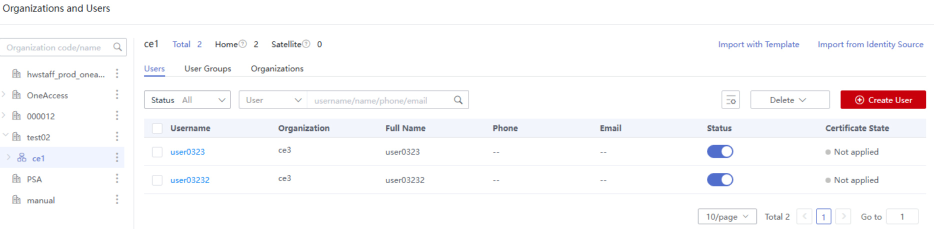
Users: 7
Created: 7, Successful: 7, Failed: 0, Active Interrupt: 0
Updated: 0, Successful: 0, Failed: 0, Active Interrupt: 0
Deleted: 0, Successful: 0, Failed: 0, Active Interrupt: 0

Organizations: 4
Created: 4 Successful: 4, Failed: 0, Active Interrupt: 0
Updated: 0 Successful: 0, Failed: 0, Active Interrupt: 0
Deleted: 0 Successful: 0, Failed: 0, Active Interrupt: 0

Created	Object	Name	Operation	Error Message	Event Status
2024-09-24 14:40:13	Organizations	[redacted]	Create		Successful
2024-09-24 14:40:13	Organizations	ce1	Create		Successful
2024-09-24 14:40:13	Organizations	ce2	Create		Successful
2024-09-24 14:40:14	Organizations	ce3	Create		Successful

  c. View the synchronized users and organizations on the **Organizations and Users** page.

Figure 2-2 Viewing synchronized data



Username	Organization	Full Name	Phone	Email	Status	Certificate State
user0323	ce3	user0323	--	--		Not applied
user03232	ce3	user03232	--	--		Not applied

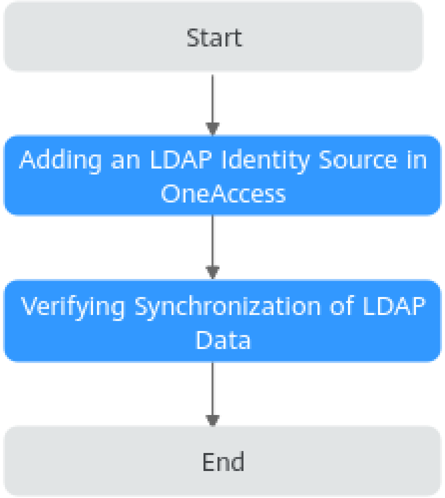
- Scheduled synchronization: If you have configured the time for scheduled synchronization in the **Advanced Settings** section of the **Import Settings** tab page, view the records on the **Scheduled Synchronization** page.

2.2 Integrating LDAP

Lightweight Directory Access Protocol (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. OneAccess allows you to import user and organization information from LDAP and synchronize the information in real time via LDAPv3.

This section describes how to integrate an LDAP identity source with OneAccess.

Configuration Process


Start
Adding an LDAP Identity Source in OneAccess
Verifying Synchronization of LDAP Data
End

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

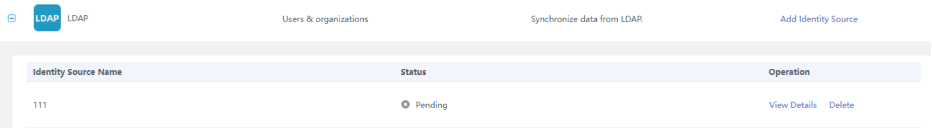
Configure parameters of the LDAP identity source in OneAccess to ensure that OneAccess can synchronize data from your LDAP server.

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**.

Step 2 Configure import settings.

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



Identity Source Name	Status	Operation
111	○ Pending	View Details Delete

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.

Table 2-5 Basic settings

Parameter	Description
* Host	Host name or IP address of the LDAP server. **NOTE** OneAccess can be accessed only over public networks. Provide the public network address of your LDAP server.
*TCP Port	TCP/IP port of the LDAP server. The default port is **636**.
SSL	Default value: **true**, which indicates that SSL is used to connect the LDAP server.
StartTLS	Whether to enable startTLS for encrypted communication. ▪ **true**: StartTLS is enabled, and SSL cannot be set to **true**. ▪ **false**: Disable StartTLS.
Verifying certificate	Whether to verify the certificate. This parameter is valid only when SSL or StartTLS is set to **true**. **true**: Verify the certificate. **false**: Do not verify the certificate. The certificate must be authenticated by the public network. Self-signed certificates cannot be used.
Protocol Version	Default value: **TLSv1.2**. Recommended: **TLSv1.3** and **TLSv1.2**.
Principal	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 principal account.

Parameter	Description
* Base Contexts	One or more root 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**.
UID Attribute	Name of the LDAP attribute mapped to the UID attribute.
Account Object Classes	One or more object classes to be used when a new user object is created in the LDAP tree. If you enter multiple object classes, each item occupies a line. Do not use commas (,) or semicolons (;) to separate multiple object classes. Some object classes may require you to specify all object classes in the class hierarchy.

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

Table 2-6 Optional settings

Parameter	Description
Domain	If a domain name exists, it should be excluded from the reclaimed username. If there are multiple domain names, separate them with commas (,). The default user name excludes the domain name.
Account Username Attributes	Saves one or more attributes of an account username. During authentication, these attributes are used to search for the LDAP entry of the username to be authenticated.
Organization Object Classes	One or more object classes that will be used when a new organization object is created in the LDAP tree. If you enter multiple object classes, each item occupies a line. Do not use commas (,) or semicolons (;) to separate multiple object classes. Some object classes may require you to specify all object classes in the class hierarchy.

Parameter	Description
Organization Name Attributes	Stores one or more attributes of the organization name. During authentication, these attributes are used to search for the LDAP entry of the organization name to be authenticated.
Failover Servers	Lists all servers that will be used for failover when the preferred server fails. If the preferred server fails, JNDI will connect to the next available server in the list. Lists all servers in the "**ldap://ldap.example.com:389/**" format (compliant with the standard LDAP v3 URL described in RFC 2255). Only the host and port parts of the URL are relevant in this setting.
Password Attribute	Name of the LDAP attribute used to store passwords. When the password of a user is changed, a new password will be set for this attribute.
LDAP Filter	Optional LDAP filter used to control the accounts returned from LDAP resources. If no filter is specified, only accounts containing all specified object classes are returned.
Password Hash Algorithm	Algorithm used by the identity system to hash passwords. Currently, **SSHA**, **SHA**, **SMD5**, and **MD5** are supported. A null value indicates that the system does not hash the password. Unless the LDAP server performs hashing (Netscape Directory Server and iPlanet Directory Server perform hashing), this will result in plaintext passwords being stored in LDAP.
Respect Resource Password Policy Change-After-Reset	If this resource is specified in the login module (i.e., this resource is the passing verification target) and the password policy of the resource is configured to change after reset, users who have reset the resource account password for management purpose need to change the password after successful verification.
Use VLV Controls	Whether to force the use of VLV controls on standard LDAP controls. The default value is **false**.
VLV Sort Attribute	Sorting attribute used for VLV indexes on resources.
Read Schema	If the value is **TRUE**, the connector reads the schema from the server. If **FALSE**, the connector provides a default schema based on the object class in the configuration. To use the extended object class, this attribute must be set to **TRUE**.
Base Contexts to Synchronize	One or more starting points in the LDAP tree that are used to determine whether changes should be synchronized. If this attribute is not set, the base context attribute is used to synchronize changes.

Parameter	Description
Object Classes to Synchronize	Object classes to be synchronized. The change log is for all objects; it filters updates based on the listed object classes. You should not list the superclasses of an object class unless you want to synchronize the object with any superclass value. For example, if only the **inetOrgPerson** object should be synchronized, but the superclasses (**person**, **organizationalperson**, and **top**) of **inetOrgPerson** should be filtered out, only **inetOrgPerson** should be listed here. All objects in LDAP are derived subclasses of **top**. Therefore, **top** should never be listed. Otherwise, no object can be filtered.
Attributes to Synchronize	Name of the attribute to be synchronized. When this option is set, if updates in the change log do not update any named attributes, these updates are ignored. For example, if only **department** is listed, only changes that affect **department** are processed and all other updates are ignored. If you leave it blank (default setting), all changes are processed.
Filter change mode	Directory administrator name (DN) used to filter changes. Filters all changes whose **modifiersName** attributes match the entries in the list. To avoid loops, the standard value is set to the administrator name used by the adapter. The entry should be in the **cn=Directory Manager** format.
AD Filter for Accounts to Synchronize	Optional LDAP filter used for synchronizing objects. Because the change log applies to all objects, this filter updates only the objects that meet the specified filter criteria. If a filter is specified, the object is synchronized only when the object meets the filter conditions and contains the synchronized object class.
Change Log Block Size	Number of change log entries obtained by each query.
Change Number Attribute	The name of the change number attribute in the change log entry.
Filter with Or Instead of And	Typically, the filter used to obtain change log entries is to retrieve change entries over a period of time based on the AND condition. If this attribute is set, the filter filters with the OR condition instead with the required number of changes.
Remove Log Entry Object Class from Filter	If this attribute is set (default), the filter used to obtain change log entries will not contain the **changeLogEntry** object class because the change log should not contain entries of other object classes.

Parameter	Description
Password Attribute to Synchronize	Name of the password attribute to be synchronized during password synchronization.
Status Management Class	Class used to manage the enabling/disabling status. If no class is specified, identity status management cannot be performed.
Retrieve Passwords with Search	Whether to retrieve the user password during search. Default value: **No**.
DN Attribute	DN attribute name of an item. The default value is **entryDN**.
LDAP Filter	Optional LDAP filter that controls the groups returned from LDAP resources. If no filter is specified, only groups containing all specified object classes are returned.
Read Timeout (ms)	Time for waiting for a response. If no response is received within the specified time, the read attempt is aborted. If the value is **0** or less than **0**, there is no limit.
Connection Timeout (ms)	Waiting time for opening a new server connection. The value **0** indicates that the TCP network timeout will be used, which may be several minutes. If the value is less than **0**, there is no limit.
Account DN Prefix	The default value is **cn**. You can also set it to another attribute name used as the DN prefix, such as uid.

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

Table 2-7 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	The default value is 20%. This is a customizable protection mechanism provided by the platform. When the number of data records disabled or deleted by the upstream identity source application exceeds the threshold, the platform will not disable or delete the data synchronously after receiving the instruction.

Parameter	Description
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.
Update Organization	Enabled by default, indicating that organizations in OneAccess that match those synchronized from the identity source will be updated. To ensure data accuracy, keep this option enabled.
Delete Organization	After organization data is synchronized from the LDAP to OneAccess, if you want to delete organizations from the LDAP, OneAccess compares the number of deleted organizations with the configured deletion threshold. If the ratio of the number of deleted organizations to the total number of data records synchronized last time is greater than the threshold, the deletion fails; if the ratio of the number of deleted organizations to the total number of data records synchronized last time is less than the threshold, the deletion is successful.
User Matching	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.

Parameter	Description
Delete User	After LDAP user data is successfully synchronized to OneAccess, if you want to delete a user from LDAP, OneAccess compares the number of deleted users with the configured deletion threshold. If the ratio of the number of deleted users to the total number of users synchronized last time is greater than the threshold, the deletion fails; if the ratio of the number of deleted users to the total number of data records synchronized last time is less than the threshold, the deletion is successful.

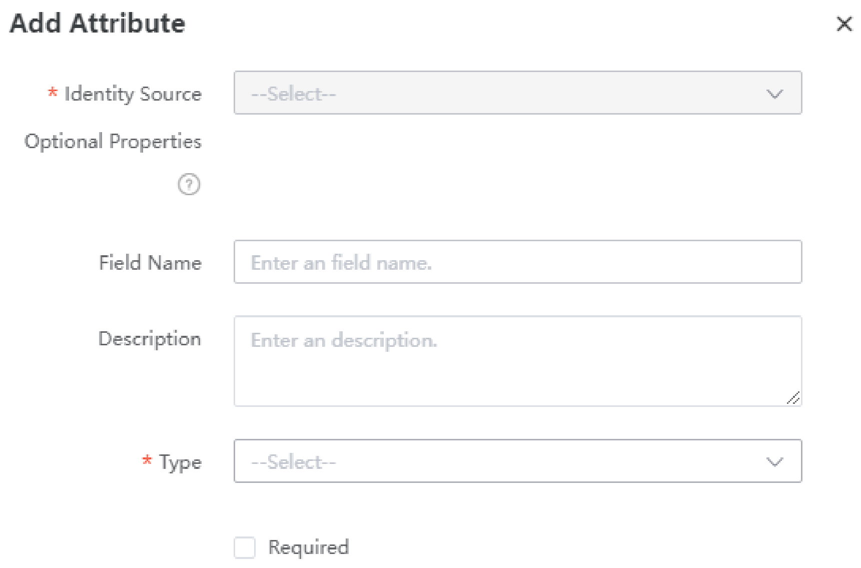
Step 3 (Optional) Set the object models.

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

Table 2-8 Object model parameters

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

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



* Identity Source: --Select--

Optional Properties

Field Name: Enter an field name.

Description: Enter an description.

* Type: --Select--

□ Required

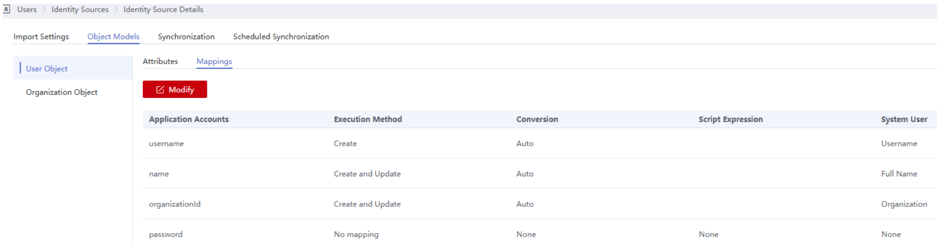
b. Select the optional attributes of the identity source, and enter the display tag and description.

c. Select a type. When **Type** is set to **Text**, you need to set **Format**.

d. Set whether the attribute is mandatory and click **OK**. The attribute is added.

- Set the mapping rule.

  On the **Mapping Definition** tab page, click **Modify**. Set the conversion mode, script expression mode, execution mode, and system user for the mapping rule.



Application Accounts	Execution Method	Conversion	Script Expression	System User
username	Create	Auto		Username
name	Create and Update	Auto		Full Name
organizationId	Create and Update	Auto		Organization
password	No mapping	None	None	None

----End

Verifying Synchronization of LDAP Data

- Synchronization via import

  a. In the LDAP identity source list, click **View Details** in the row that contains the target identity source. Click the **Synchronization** tab, and click **Execute**. OneAccess synchronizes user and organization data from the LDAP identity source, and generates operation records.

  b. Click **View Details** in the row that contains the target record to view details.

  c. View the synchronized users and organizations on the **Organizations and Users** page.

- 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.

3 Application Integration

3.1 Logging In to the Huawei Cloud Through User Portal

3.1.1 Introduction

Huawei Cloud supports single sign-on (SSO) based on SAML and OpenID Connect (OIDC). After the enterprise administrator configures Huawei Cloud and OneAccess, common users can log in to the OneAccess user portal to access Huawei Cloud console or a specific Huawei Cloud application without entering a password.

Prerequisites

- Your browser can access the Huawei Cloud console.
- You have permissions to access the administrator portal.
- You have a HUAWEI ID. For details about how to register one, see **Registering an Account and Completing Real-Name Authentication**.

3.1.2 Logging In to Single Huawei Cloud Account via OneAccess Without Password (SAML - Virtual User SSO)

This section uses SAML as an example to describe how to use OneAccess to log in to a Huawei Cloud account without entering a password. For details about Huawei Cloud identity providers (IdPs), see **Identity Provider Overview**.

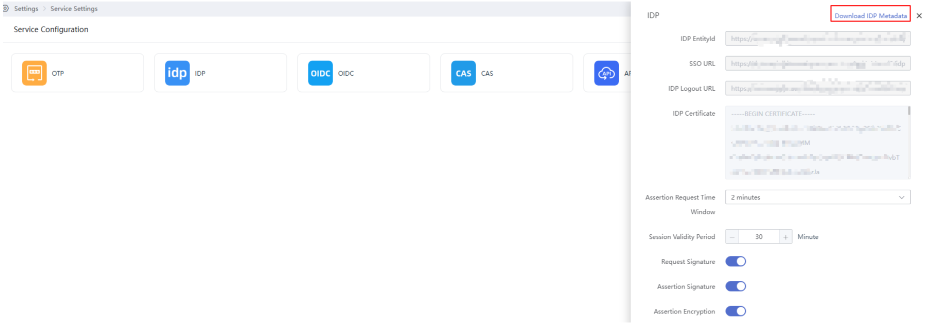
Creating an IdP on Huawei Cloud

Create an IdP and configure the metadata file on the Huawei Cloud console.

Step 1 Log in to the OneAccess administrator portal and download the metadata file of OneAccess.

1. Log in to the administrator portal.

2. On the top navigation bar, choose **Settings** > **Service Settings**.
3. On the displayed page, click **IDP**.
4. On the IdP configuration page, click **Download IDP Metadata** in the upper right. The metadata file is automatically saved.



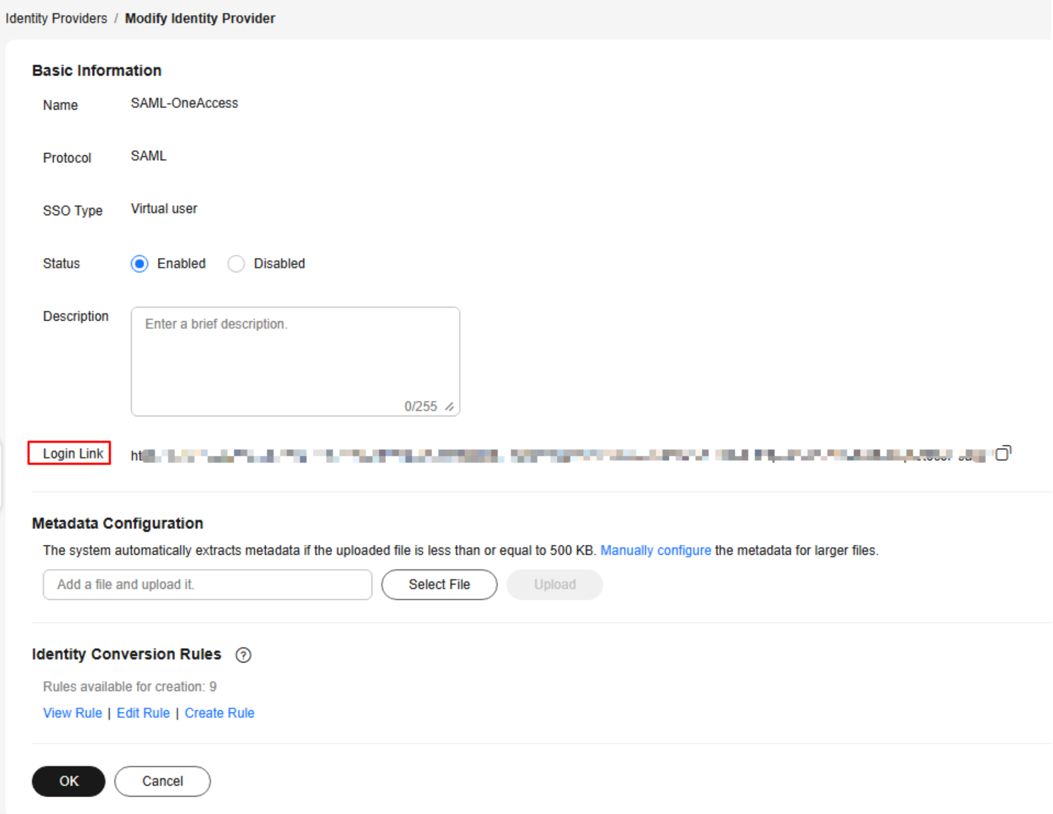
IDP EntityId [redacted]
SSO URL [redacted]
IDP Logout URL [redacted]
IDP Certificate -----BEGIN CERTIFICATE----- [redacted]
Assertion Request Time Window: 2 minutes
Session Validity Period: 30 Minute
Request Signature
Assertion Signature
Assertion Encryption

Step 2 Create an IdP of the virtual user SSO type. For details, see **Creating an IdP Entity on Huawei Cloud**.

📖 NOTE

- The IdP name must be unique. You are advised to use the domain name.
- For details about virtual user SSO, see **Application Scenarios of Virtual User SSO and IAM User SSO**.
- A Huawei Cloud account can have only one IdP type: either IAM user SSO or virtual user SSO.

Step 3 Obtain the Huawei Cloud login link.


Identity Providers / Modify Identity Provider

Basic Information

Name: SAML-OneAccess

Protocol: SAML

SSO Type: Virtual user

Status: ● Enabled ○ Disabled

Description: Enter a brief description. 0/255

Login Link: ht[redacted]

Metadata Configuration

The system automatically extracts metadata if the uploaded file is less than or equal to 500 KB. Manually configure the metadata for larger files.

Add a file and upload it.
Select File
Upload

Identity Conversion Rules

Rules available for creation: 9

Step 4 Configure the metadata file of the OneAccess IdP on Huawei Cloud. For details, see **Configuring the Metadata File of the Identity Provider**.

Step 5 Configure identity conversion rules on Huawei Cloud so that OneAccess users can access cloud services and resources. For details, see **Configure Identity Conversion Rules**.

Assuming all OneAccess users belong to the same IAM user group, once they log in to Huawei Cloud, their IAM username will appear as their OneAccess username. The conversion rule is as follows:

```
[
  {
    "remote": [
      {
        "type": "name"
      }
    ],
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      },
      {
        "group": {
          "name": "admin"
        }
      }
    ]
  }
]
```

remote indicates the information mapped from OneAccess to IAM. Obtain the **name** field. For details about the mapping fields, see **Step 2**.

local indicates the local IAM information, **user** indicates the IAM user, **name** indicates the displayed IAM username, and **{0}** indicates the first field in **remote**. **group** indicates the IAM user group, indicating that all users are mapped to the **admin** user group and have all permissions.

Similarly, you can add multiple fields to **remote** and set one of the fields to the user group name so that different users correspond to different user groups.

```
[
  {
    "remote": [
      {
        "type": "name"
      },
      {
        "type": "Roles"
      }
    ],
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      },
      {
        "groups": "{1}"
      }
    ]
  }
]
```

remote indicates that the **Roles** field is mapped additionally. (You can use the custom field in the user attribute definition.) It can be a single value or multiple values.

local indicates that **groups** is used and can be mapped to multiple IAM user groups. The second **Roles** field in **remote** is used.

----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 OneAccess administrator portal, and choose **Resources** > **Applications**.
2. Click **Add Pre-integrated Application** under **Pre-integrated Applications**.
3. On the **Add Pre-integrated Application** page, click **Huawei Cloud**.
4. On the **Add Application** page, confirm the general information, and click **Next**.
5. On the **Authentication Parameters** page, click **Import SP Metadata**, click **Select File**, select the Huawei Cloud metadata file, and click **Open**. The system automatically extracts the metadata.

   NOTE

   – Pre-integrated applications are available for professional edition users only. Basic edition users need to create custom applications by referring to **Adding an Application** and then perform operations in **Step 1.5**.

   – To obtain the Huawei Cloud metadata file, visit **https://auth.huaweicloud.com/authui/saml/metadata.xml**, and save the metadata as **SP-metadata.xml**.

   – OneAccess allows you to configure metadata by selecting a file or configuring parameters. For details, see **Configuring a Metadata File**.
6. When the **Select File** button changes to **√**, the system has extracted the metadata. Click **Next**.
7. On the authentication integration page, click **Modify** on the **Parameters** tab page, and replace **/saml/LogoutServiceHTTPRedirect** in the value of **Single Logout URL** with **/logout**.

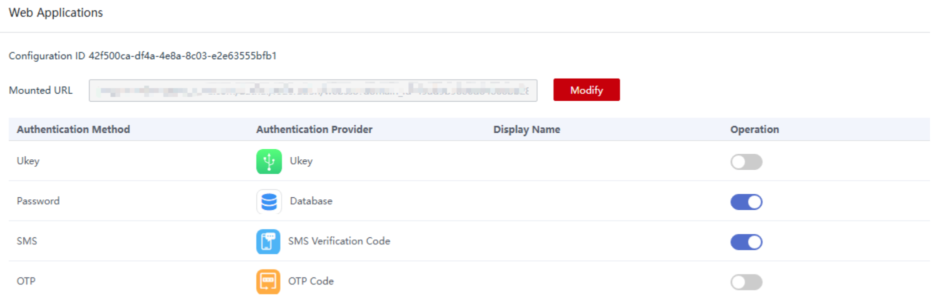
Step 2 Configure mappings between OneAccess and Huawei Cloud.

1. Click the added Huawei Cloud application. On the application information page, click the application icon to go to the application details page.
2. Choose **Authentication Integration** > **Mappings**, and click **Add Mapping** to configure mappings. For details about the parameters, see **Configuring Mappings and Authorizing Users**.

Step 3 Configure the Huawei Cloud login entry in OneAccess.

On the Huawei Cloud application details page, choose **Login Settings** > **Web Applications**, click **Modify**, replace the URL with the login URL obtained in **Step 3**, and click **OK** to save it.

Figure 3-1 Editing the URL



Web Applications

Configuration ID 42f500ca-df4a-4e8a-8c03-e2e63555bfb1

Mounted URL [redacted]

Authentication Method	Authentication Provider	Display Name	Operation
Ukey	Ukey		○
Password	Database		●
SMS	SMS Verification Code		●
OTP	OTP Code		○

NOTE

To redirect to a specific service page on the Huawei Cloud console, combine the login link of the identity provider created on Huawei Cloud and enter the combined URL. The following takes CodeArts as an example:

Login link of the identity provider created on Huawei Cloud: **https://auth.huawei.com/authui/federation/websso?domain_id=e35f94************14839c&idp=SAML-OneAccess&protocol=saml**

CodeArts service address: https://console-intl.huaweicloud.com/devcloud/?locale=en-us#

If the service address contains the **agencyId=***&** field, delete the field, use **&service=** to combine the two addresses, and enter the combined address in the URL.

https://auth.huawei.com/authui/federation/websso?domain_id=e35f94************14839c&idp=SAML-OneAccess&protocol=saml&service=https://console-intl.huaweicloud.com/devcloud/?locale=zh-cn#

Step 4 Grant Huawei Cloud access permissions to users in OneAccess.

On the Huawei Cloud application details page, choose **Authorization** > **Application Accounts**, click the button for adding accounts, select required accounts, and click **Save**. The selected accounts can access Huawei Cloud via OneAccess without a password.

----End

Logging In as a User

Users with Huawei Cloud access permissions can easily access the Huawei Cloud console with a single click after logging in to the OneAccess user portal.

3.1.3 Logging In to Multiple Huawei Cloud Accounts via OneAccess Without Password (SAML - Virtual User SSO)

This section uses SAML as an example to describe how to use OneAccess to log in to multiple Huawei Cloud account without entering a password. For details about Huawei Cloud identity providers (IdPs), see **Identity Provider Introduction**.

Creating an IdP on Huawei Cloud

Create an IdP and configure the metadata file on the Huawei Cloud console.

Step 1 Log in to the OneAccess administrator portal and download the metadata file of OneAccess.

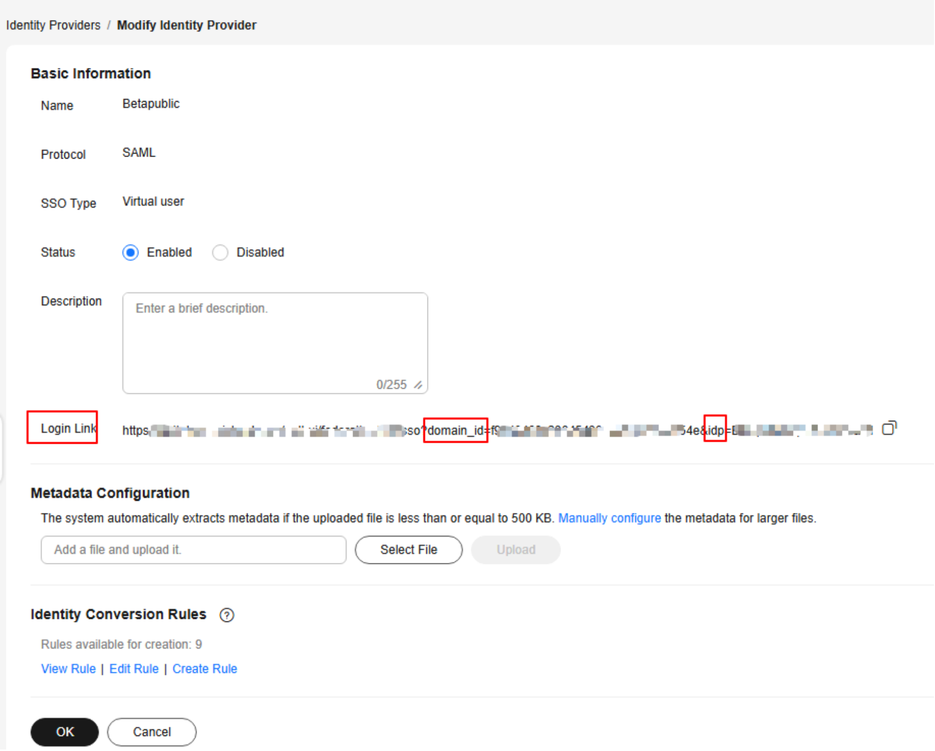
1. Log in to the administrator portal.
2. On the top navigation bar, choose **Settings** > **Service Settings**.
3. On the displayed page, click **IDP**.
4. On the IdP configuration page, click **Download IDP Metadata** in the upper right. The metadata file is automatically saved.

Step 2 Create an IdP of the virtual user SSO type. For details, see **Creating an IdP Entity on Huawei Cloud**.

NOTE

- The IdP name must be unique. You are advised to use the domain name.
- For details about virtual user SSO, see **Application Scenarios of Virtual User SSO and IAM User SSO**.
- A Huawei Cloud account can have only one IdP type: either IAM user SSO or virtual user SSO.

Step 3 Obtain the values of **domain_id** and **idp** in the Huawei Cloud login link.



Identity Providers / Modify Identity Provider

Basic Information

Name: Betapublic

Protocol: SAML

SSO Type: Virtual user

Status: ● Enabled ○ Disabled

Description: Enter a brief description. 0/255

Login Link: https[redacted]sso?domain_id=[redacted]&idp=[redacted]

Metadata Configuration

The system automatically extracts metadata if the uploaded file is less than or equal to 500 KB. Manually configure the metadata for larger files.

Add a file and upload it. | Select File | Upload

Identity Conversion Rules

Rules available for creation: 9

View Rule | Edit Rule | Create Rule

OK | Cancel

Step 4 Configure the metadata file of the OneAccess IdP on Huawei Cloud. For details, see **Configuring the Metadata File of the Identity Provider**.

Step 5 Configure identity conversion rules on Huawei Cloud so that OneAccess users can access cloud services and resources. For details, see **Configure Identity Conversion Rules**.

Assuming all OneAccess users belong to the same IAM user group, once they log in to Huawei Cloud, their IAM username will appear as their OneAccess username. The conversion rule is as follows:

```
[
 {
  "remote": [
   {
    "type": "name"
   }
  ],
  "local": [
   {
    "user": {
     "name": "{0}"
    }
   },
   {
    "group": {
     "name": "admin"
    }
   }
  ]
 }
]
```

remote indicates the information mapped from OneAccess to IAM. Obtain the **name** field. For details about the mapping fields, see **Step 2**.

local indicates the local IAM information, **user** indicates the IAM user, **name** indicates the displayed IAM username, and **{0}** indicates the first field in **remote**. **group** indicates the IAM user group, indicating that all users are mapped to the **admin** user group and have all permissions.

Similarly, you can add multiple fields to **remote** and set one of the fields to the user group name so that different users correspond to different user groups.

```
[
 {
  "remote": [
   {
    "type": "name"
   },
   {
    "type": "Roles"
   }
  ],
  "local": [
   {
    "user": {
     "name": "{0}"
    }
   },
   {
    "groups": "{1}"
   }
  ]
 }
]
```

remote indicates that the **Roles** field is mapped additionally. (You can use the custom field in the user attribute definition.) It can be a single value or multiple values.

local indicates that **groups** is used and can be mapped to multiple IAM user groups. The second **Roles** field in **remote** is used.

Step 6 Repeat **Step 2** to **Step 5** for other Huawei Cloud accounts.

----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 OneAccess administrator portal, and choose **Resources** > **Applications**.
2. Click **Add Pre-integrated Application** under **Pre-integrated Applications**.
3. On the **Add Pre-integrated Application** page, click **Huawei Cloud**.
4. On the **Add Application** page, confirm the general information, and click **Next**.
5. On the **Authentication Parameters** page, click **Import SP Metadata**, click **Select File**, select the Huawei Cloud metadata file, and click **Open**. The system automatically extracts the metadata.

   NOTE

   – Pre-integrated applications are available for professional edition users only. Basic edition users need to create custom applications by referring to **Adding an Application** and then perform operations in **Step 1.5**.

   – To obtain the Huawei Cloud metadata file, visit **https://auth.huaweicloud.com/authui/saml/metadata.xml**, and save the metadata as **SP-metadata.xml**.

   – OneAccess allows you to configure metadata by selecting a file or configuring parameters. For details, see **Configuring a Metadata File**.
6. When the **Select File** button changes to **√**, the system has extracted the metadata. Click **Next**.
7. On the authentication integration page, click **Modify** on the **Parameters** tab page, and replace **/saml/LogoutServiceHTTPRedirect** in the value of **Single Logout URL** with **/logout**.

Step 2 Configure mappings between OneAccess and Huawei Cloud.

1. Click the added Huawei Cloud application. On the application information page, click the application icon to go to the application details page.
2. Choose **Authentication Integration** > **Mappings**, and click **Add Mapping** to configure mappings. For details about the parameters, see **Configuring Mappings and Authorizing Users**.
3. Choose **Authentication Integration** > **Mappings**, click **Add Mapping**, and set **Application Attribute** to **IAM_SAML_Attributes_identityProviders**, **Mapping Type** to **Fixed attribute value**, and **Fixed attribute value** to **iam::*{domain_id}*:identityProvider:*{idp_id}***. *{domain_id}* indicates the domain ID obtained in **Step 3**, and *{idp_id}* indicates the ID obtained in **Step 3**. Separate multiple Huawei Cloud accounts with semicolons (;), so that you can choose to redirect to a target account. If there are two Huawei Cloud accounts, the values are as follows:

   iam::657ba0e***********19fd684d8758c:identityProvider:SAML-IAM;iam::e35f949b3*********2b79ba14839c:identityProvider:SAML-OneAccess
4. (Optional) Click **Add Mapping**, and set **Application Attribute** to **IAM_SAML_Attributes_redirect_url**, **Mapping Type** to **Fixed attribute value**, and **Fixed attribute value** to a specific service page on the Huawei Cloud Console (if the service address contains the **agencyId=***&** field, delete this

field), so that the SSO can be redirected to the service page. If no service page is specified in the value, the Huawei Cloud home page is displayed by default.

Step 3 Grant Huawei Cloud access permissions to users in OneAccess.

On the Huawei Cloud application details page, choose **Authorization** > **Application Accounts**, click the button for adding accounts, select required accounts, and click **Save**. The selected accounts can access Huawei Cloud via OneAccess without a password.

----End

Logging In as a User

Users with Huawei Cloud access permissions can access the Huawei Cloud console with a single click after logging in to the OneAccess user portal and selecting an IdP.

3.1.4 Logging In to Single Huawei Cloud Account via OneAccess Without Password (SAML - IAM User SSO)

This section uses SAML as an example to describe how to use OneAccess to log in to a Huawei Cloud account without entering a password. For details about Huawei Cloud identity providers (IdPs), see **Identity Provider Overview**.

Creating an IdP on Huawei Cloud

Create an IdP and configure the metadata file on the Huawei Cloud console.

Step 1 Log in to the OneAccess administrator portal and download the metadata file of OneAccess.

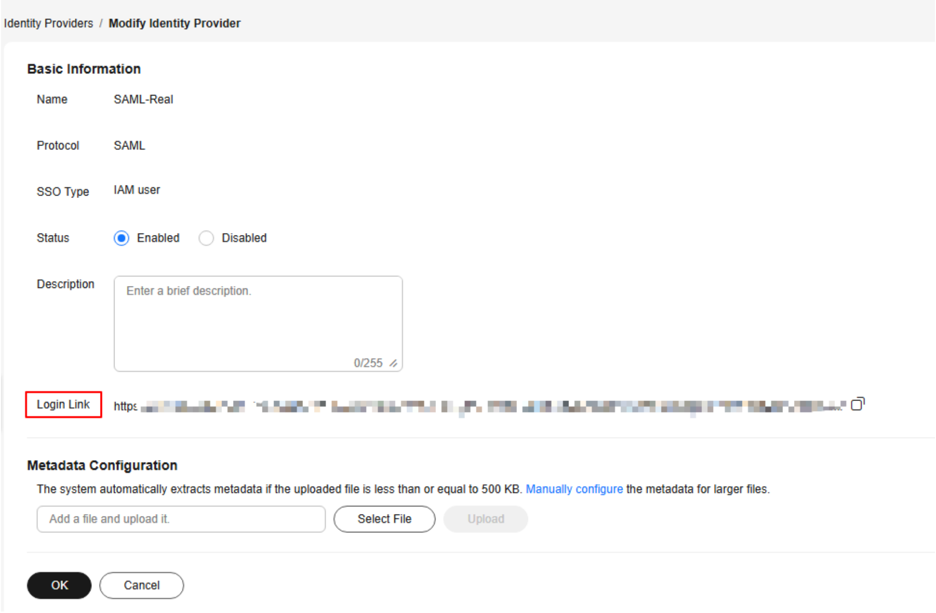
1. Log in to the administrator portal.
2. On the top navigation bar, choose **Settings** > **Service Settings**.
3. On the displayed page, click **IDP**.
4. On the IdP configuration page, click **Download IDP Metadata** in the upper right. The metadata file is automatically saved.

Step 2 Create an IdP of the IAM user SSO type. For details, see **Creating an IdP Entity on Huawei Cloud**.

NOTE

- The IdP name must be unique. You are advised to use the domain name.
- For details about IAM user SSO, see **Application Scenarios of Virtual User SSO and IAM User SSO**.
- A Huawei Cloud account can have only one IdP type: either IAM user SSO or virtual user SSO.

Step 3 Obtain the Huawei Cloud login link.



Identity Providers / Modify Identity Provider

Basic Information

Name SAML-Real

Protocol SAML

SSO Type IAM user

Status ● Enabled ○ Disabled

Description Enter a brief description. 0/255

Login Link https[redacted]

Metadata Configuration

The system automatically extracts metadata if the uploaded file is less than or equal to 500 KB. Manually configure the metadata for larger files.

Step 4 Configure the metadata file of the OneAccess IdP on Huawei Cloud. For details, see **Configuring the Metadata File of the Identity Provider**.

Step 5 Configure an external identity ID for the IAM user on Huawei Cloud by referring to **Configuring an External Identity ID** to establish the mapping between the OneAccess user and the IAM user.

----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 OneAccess administrator portal, and choose **Resources** > **Applications**.
2. Click **Add Pre-integrated Application** under **Pre-integrated Applications**.
3. On the **Add Pre-integrated Application** page, click **Huawei Cloud**.
4. On the **Add Application** page, confirm the general information, and click **Next**.
5. On the **Authentication Parameters** page, click **Import SP Metadata**, click **Select File**, select the Huawei Cloud metadata file, and click **Open**. The system automatically extracts the metadata.

NOTE

- Pre-integrated applications are available for professional edition users only. Basic edition users need to create custom applications by referring to **Adding an Application** and then perform operations in **Step 1.5**.
- To obtain the Huawei Cloud metadata file, visit **https://auth.huaweicloud.com/authui/saml/metadata.xml**, and save the metadata as **SP-metadata.xml**.
- OneAccess allows you to configure metadata by selecting a file or configuring parameters. For details, see **Configuring a Metadata File**.

6. When the **Select File** button changes to **√**, the system has extracted the metadata. Click **Next**.
7. On the authentication integration page, click **Modify** on the **Parameters** tab page, and replace **/saml/LogoutServiceHTTPRedirect** in the value of **Single Logout URL** with **/logout**.

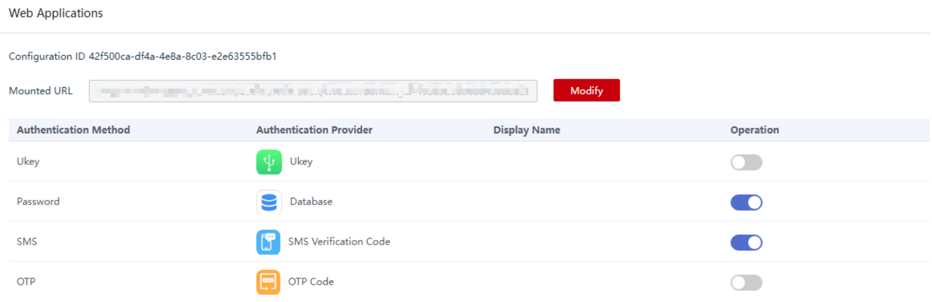
Step 2 Configure mappings between OneAccess and Huawei Cloud.

1. Click the added Huawei Cloud application. On the application information page, click the application icon to go to the application details page.
2. Choose **Authentication Integration** > **Mappings**.
3. Click **Add Mapping** and add a mapping whose application attribute is **IAM_SAML_Attributes_xUserId** to establish the attribute mapping between OneAccess and Huawei Cloud. The mapping object can be an existing attribute of the OneAccess user or a new custom attribute. The mapping object must be the same as the external identity ID of the IAM user added in **Step 5**.

Step 3 Configure the Huawei Cloud login entry in OneAccess.

On the Huawei Cloud application details page, choose **Login Settings** > **Web Applications**, click **Modify**, replace the URL with the login URL obtained in **Step 3**, and click **OK** to save it.

Figure 3-2 Editing the URL



Web Applications

Configuration ID 42f500ca-df4a-4e8a-8c03-e2e63555bfb1

Mounted URL [redacted] Modify

Authentication Method	Authentication Provider	Display Name	Operation
Ukey	Ukey		○
Password	Database		●
SMS	SMS Verification Code		●
OTP	OTP Code		○

NOTE

To redirect to a specific service page on the Huawei Cloud console, combine the login link of the identity provider created on Huawei Cloud and enter the combined URL. The following takes CodeArts as an example:

Login link of the identity provider created on Huawei Cloud: **https://auth.huawei.com/authui/federation/websso?domain_id=e35f94************14839c&idp=SAML-OneAccess&protocol=saml**

CodeArts service address: https://console-intl.huaweicloud.com/devcloud/?locale=en-us#

If the service address contains the **agencyId=***&** field, delete the field, use **&service=** to combine the two addresses, and enter the combined address in the URL.

https://auth.huawei.com/authui/federation/websso?domain_id=e35f94************14839c&idp=SAML-OneAccess&protocol=saml&service=https://console-intl.huaweicloud.com/devcloud/?locale=zh-cn#

Step 4 Grant Huawei Cloud access permissions to users in OneAccess.

On the Huawei Cloud application details page, choose **Authorization** > **Application Accounts**, click the button for adding accounts, select required accounts, and click **Save**. The selected accounts can access Huawei Cloud via OneAccess without a password.

----End

Logging In as a User

Users with Huawei Cloud access permissions can easily access the Huawei Cloud console with a single click after logging in to the OneAccess user portal.

3.1.5 Logging In to Multiple Huawei Cloud Accounts via OneAccess Without Password (SAML - IAM User SSO)

This section uses SAML as an example to describe how to use OneAccess to log in to multiple Huawei Cloud account without entering a password. For details about Huawei Cloud identity providers (IdPs), see **Identity Provider Overview**.

Creating an IdP on Huawei Cloud

Create an IdP and configure the metadata file on the Huawei Cloud console.

Step 1 Log in to the OneAccess administrator portal and download the metadata file of OneAccess.

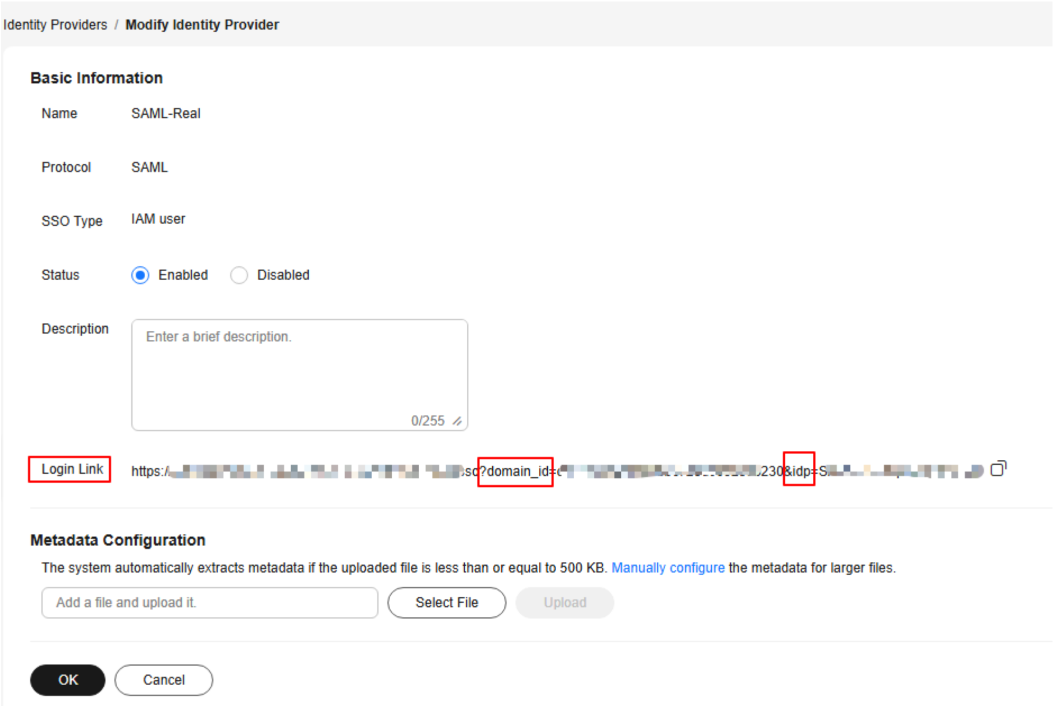
1. Log in to the administrator portal.
2. On the top navigation bar, choose **Settings** > **Service Settings**.
3. On the displayed page, click **IDP**.
4. On the IdP configuration page, click **Download IDP Metadata** in the upper right. The metadata file is automatically saved.

Step 2 Create an IdP of the IAM user SSO type. For details, see **Creating an IdP Entity on Huawei Cloud**.

NOTE

- The IdP name must be unique. You are advised to use the domain name.
- For details about IAM user SSO, see **Application Scenarios of Virtual User SSO and IAM User SSO**.
- A Huawei Cloud account can have only one IdP type: either IAM user SSO or virtual user SSO.

Step 3 Obtain the Huawei Cloud login link, and the values of **domain_id** and **idp**.



Identity Providers / Modify Identity Provider

Basic Information

Name SAML-Real

Protocol SAML

SSO Type IAM user

Status ● Enabled ○ Disabled

Description Enter a brief description. 0/255

Login Link https:/[redacted]sc?domain_id=[redacted]230&idp=S[redacted]

Metadata Configuration

The system automatically extracts metadata if the uploaded file is less than or equal to 500 KB. Manually configure the metadata for larger files.

Step 4 Configure the metadata file of the OneAccess IdP on Huawei Cloud. For details, see **Configuring the Metadata File of the Identity Provider**.

Step 5 Configure an external identity ID for the IAM user on Huawei Cloud by referring to **Configuring an External Identity ID** to establish the mapping between the OneAccess user and the IAM user.

Step 6 Repeat **Step 2** to **Step 5** for other Huawei Cloud accounts.

----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 OneAccess administrator portal, and choose **Resources** > **Applications**.
2. Click **Add Pre-integrated Application** under **Pre-integrated Applications**.
3. On the **Add Pre-integrated Application** page, click **Huawei Cloud**.
4. On the **Add Application** page, confirm the general information, and click **Next**.
5. On the **Authentication Parameters** page, click **Import SP Metadata**, click **Select File**, select the Huawei Cloud metadata file, and click **Open**. The system automatically extracts the metadata.

NOTE

- Pre-integrated applications are available for professional edition users only. Basic edition users need to create custom applications by referring to **Adding an Application** and then perform operations in **Step 1.5**.
- To obtain the Huawei Cloud metadata file, visit **https://auth.huaweicloud.com/authui/saml/metadata.xml**, and save the metadata as **SP-metadata.xml**.
- OneAccess allows you to configure metadata by selecting a file or configuring parameters. For details, see **Configuring a Metadata File**.

6. When the **Select File** button changes to **√**, the system has extracted the metadata. Click **Next**.
7. On the authentication integration page, click **Modify** on the **Parameters** tab page, and replace **/saml/LogoutServiceHTTPRedirect** in the value of **Single Logout URL** with **/logout**.

Step 2 Configure mappings between OneAccess and Huawei Cloud.

1. Click the added Huawei Cloud application. On the application information page, click the application icon to go to the application details page.
2. Choose **Authentication Integration** > **Mappings**.
3. Click **Add Mapping** and add a mapping whose application attribute is **IAM_SAML_Attributes_xUserId** to establish the attribute mapping between OneAccess and Huawei Cloud. The mapping object can be an existing attribute of the OneAccess user or a new custom attribute. The mapping object must be the same as the external identity ID of the IAM user added in **Step 5**.
4. Click **Add Mapping**, and set **Application Attribute** to **IAM_SAML_Attributes_identityProviders**, **Mapping Type** to **Fixed attribute value**, and **Fixed attribute value** to **iam::*{domain_id}*:identityProvider:*{idp_id}***. *{domain_id}* indicates the domain ID obtained in **Step 3**, and *{idp_id}* indicates the ID obtained in **Step 3**. Use semicolons (;) to separate Huawei Cloud accounts for redirection to a target account. If there are two Huawei Cloud accounts, the values are as follows:

   iam::657ba0e***********19fd684d8758c:identityProvider:SAML-IAM;iam::e35f949b3*********2b79ba14839c:identityProvider:SAML-OneAccess
5. (Optional) Click **Add Mapping**, and set **Application Attribute** to **IAM_SAML_Attributes_redirect_url**, **Mapping Type** to **Fixed attribute value**, and **Fixed attribute value** to a specific service page on the Huawei Cloud Console (if the service address contains the **agencyId=***&** field, delete this field), so that the SSO can be redirected to the service page. If no service page is specified in the value, the Huawei Cloud home page is displayed by default.

Step 3 Grant Huawei Cloud access permissions to users in OneAccess.

On the Huawei Cloud application details page, choose **Authorization** > **Application Accounts**, click the button for adding accounts, select required accounts, and click **Save**. The selected accounts can access Huawei Cloud via OneAccess without a password.

----End

Logging In as a User

Users with Huawei Cloud access permissions can access the Huawei Cloud console with a single click after logging in to the OneAccess user portal and selecting an IdP.

3.1.6 Logging In to Huawei Cloud via OneAccess Without Password (OIDC)

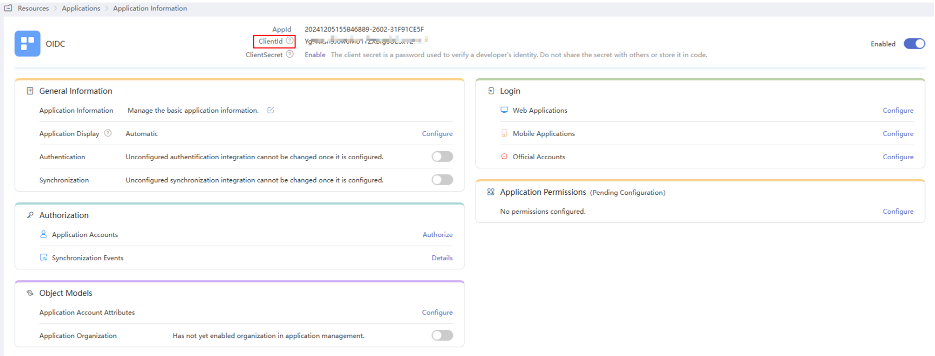
This section uses OIDC as an example to describe how to use OneAccess to log in to CodeArts on the Huawei Cloud console without entering a password.

Creating a Huawei Cloud OIDC Application

Create a Huawei Cloud OIDC application on the OneAccess administrator portal and obtain the OIDC settings to establish a trust relationship between OneAccess and Huawei Cloud.

Step 1 Add the Huawei Cloud application in OneAccess.

1. Log in to the OneAccess administrator portal, and choose **Resources** > **Applications**.
2. Click **Add Custom Application**.
3. Enter an application name and click **Save**.
4. Click the created application and copy the value of **ClientId**.



Resources > Applications > Application Information

OIDC

AppId 20241205155846889-2602-31F91CE5F
ClientId [redacted]
ClientSecret Enable The client secret is a password used to verify a developer's identity. Do not share the secret with others or store it in code.

Enabled

General Information
Application Information Manage the basic application information.
Application Display Automatic Configure
Authentication Unconfigured authentification integration cannot be changed once it is configured.
Synchronization Unconfigured synchronization integration cannot be changed once it is configured.

Authorization
Application Accounts Authorize
Synchronization Events Details

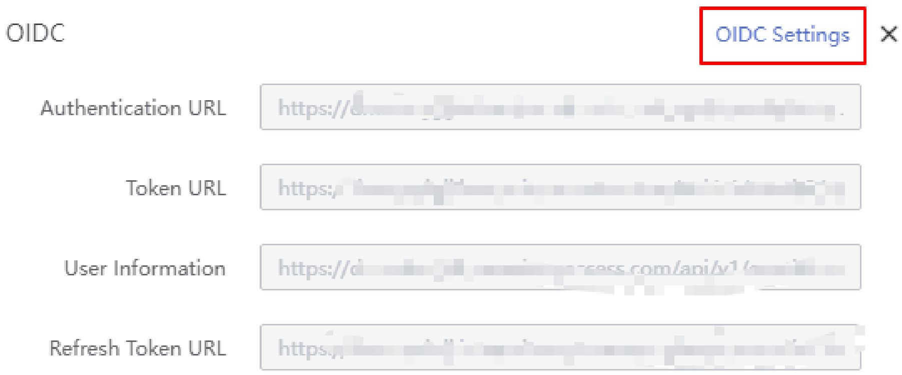
Object Models
Application Account Attributes Configure
Application Organization Has not yet enabled organization in application management.

Login
Web Applications Configure
Mobile Applications Configure
Official Accounts Configure

Application Permissions (Pending Configuration)
No permissions configured. Configure

Step 2 Obtain OIDC configurations.

1. Log in to the OneAccess administrator portal, and choose **Settings** > **Service Settings**.
2. On the displayed page, click **OIDC**.
3. Click **OIDC Settings**.



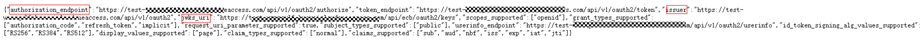
Authentication URL: https://d[redacted]

Token URL: https:/[redacted]

User Information: https://d[redacted]cess.com/api/v1/[redacted]

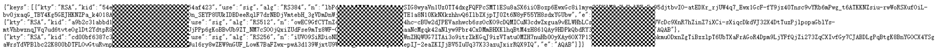
Refresh Token URL: https:/[redacted]

4. Obtain the **issuer**, **authorization_endpoint**, and **jwks_uri** addresses.



```
{"authorization_endpoint":"https://test-[redacted]eaccess.com/api/v1/oauth2/authorize","token_endpoint":"https://test-[redacted]s.com/api/v1/oauth2/token","issuer":"https://test-
[redacted]eaccess.com/api/v1/oauth2","jwks_uri":"https://t[redacted]m/api/ecb/oauth2/keys","scopes_supported":["openid"],"grant_types_supported":
["authorization_code","refresh_token","implicit"],"request_uri_parameter_supported":true,"subject_types_supported":["public"],"userinfo_endpoint":"https://test-[redacted]m/api/v1/oauth2/userinfo","id_token_signing_alg_values_supported":
["RS256","RS384","RS512"],"display_values_supported":["page"],"claim_types_supported":["normal"],"claims_supported":["sub","aud","nbf","iss","exp","iat","jti"]}
```

5. Copy the **jwks_uri** address to the address box of a browser to obtain the signing key.



```
{"keys":[{"kty":"RSA","kid":"54e[redacted]54af423","use":"sig","alg":"RS384","n":"lbPc[redacted]SIG8wyaVn1UzOTT4dxgFQFPcSMT1ESu8aSX6iiOBozp6EwxGc8i1mye[redacted]95djtbvIO-atEDXr_rjUW4q7_Ewx1GcF-fY9jz40Tnsc9vYRb6mPwg_t6ATKKNZsiu-rwWoRSXufOiL-
bv0jxaqG_TBY4Kg5GEJHKNZPa_k4018A[redacted]On_SEYP8UUkIDBDeeRqlF7drNBDjVmtebH_3gVDmDnW[redacted]TE1a8N10KkNXkzhhvQ6IlbZXjpTJ0Zt6N8yF55YH8sdxYGUbw","e":[redacted]
{"kty":"RSA","kid":"a9b2c31abbd1[redacted]"use":"sig","alg":"RS512","n":"owEC9GfCYTnZ4[redacted]4hc-cBUw2dJPEVashwcb6ssOcKO9cDQMICuN3cdwZxgua9vELWHbLCs[redacted]VcDc9XnR7hZinZ7iXCi-sXiqcDkdVJ32X4DtTuzPjlpopaGblYs-
mtVhbwznqJVq7ud6tvteOglDt2YdtpR8[redacted]JjPPp6gKoBBvUb9ZT_NM7cSOOjQxiZUdFse9mTz8WF-C[redacted]aaNcMgqk42aNlyw9Pbr4CxDMmBHXKlhqBtM4zH861QAy9HDPkQbdRY3[redacted]"AQAB"},
{"kty":"RSA","kid":"cd00bf6387c3[redacted]"use":"sig","alg":"RS256","n":"iUVO9SiRDioND[redacted]WnZHQWUG7ITAi3o9itrZkKGqJ9izVTatuOMZH7nuHbOOyXAy6OX7P1S[redacted]okmuODxnZgTiBzz1pT6UbTXaFrAGoR4Dpm9LjYFfQjZi273ZqCXIvfGy7CJABDLgPqBtgK8BnYGOCX4YSg
aWrsYdVPBlbc22K800bDTFLOvGtuRvnp[redacted]Wu16ry8wZEW9nGUF_LowK7BaFZwx-pwA3d139WjxtU9V[redacted]epIJ-2eaZKIJjBV5IuUq37X33azuJxirRQX9IQ","e":"AQAB"}]}
```

----End

Creating an IdP on Huawei Cloud

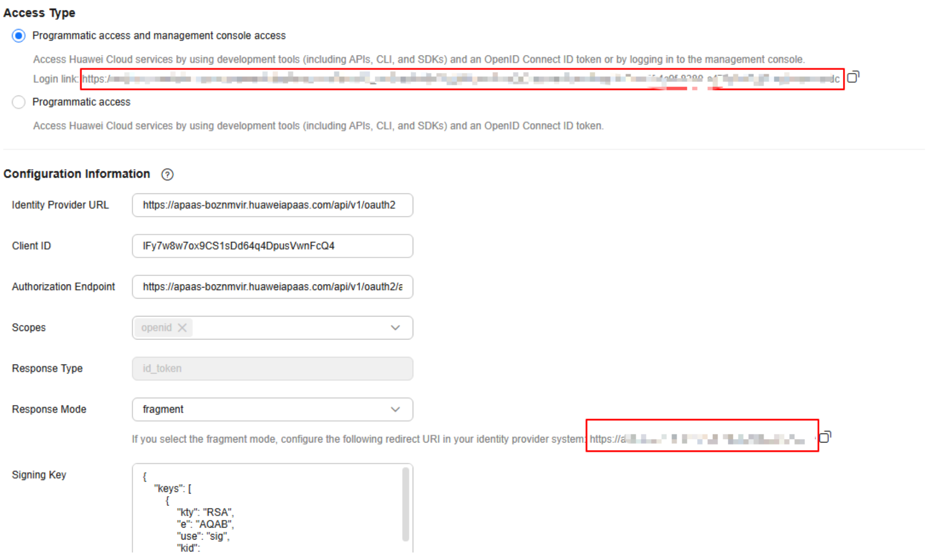
Create an IdP and configure the OneAccess application and OIDC on the Huawei Cloud console.

Step 1 Create an IdP. For details, see **Creating an IdP Entity on Huawei Cloud**.

NOTE

- The IdP name must be unique. You are advised to use the domain name.
- Specify the configuration information.
  1. **Identity Provider URL**: **issuer** address obtained in **Step 2.4**.
  2. Authorization Endpoint: **authorization_endpoint** address obtained in **Step 2.4**.
  3. Client ID: OIDC application **ClientId** obtained in **Step 1.4**.
  4. **Signing Key**: Public key (in JSON format) obtained in **Step 2.5**.

Step 2 Copy the login address and redirect URI during the configuration.



Access Type

● Programmatic access and management console access

Access Huawei Cloud services by using development tools (including APIs, CLI, and SDKs) and an OpenID Connect ID token or by logging in to the management console.

Login link: https:/[redacted]

○ Programmatic access

Access Huawei Cloud services by using development tools (including APIs, CLI, and SDKs) and an OpenID Connect ID token.

Configuration Information

Identity Provider URL	https://apaas-boznmvir.huaweiapaas.com/api/v1/oauth2
Client ID	IFy7w8w7ox9CS1sDd64q4DpusVwnFcQ4
Authorization Endpoint	https://apaas-boznmvir.huaweiapaas.com/api/v1/oauth2/a
Scopes	openid
Response Type	id_token
Response Mode	fragment

If you select the fragment mode, configure the following redirect URI in your identity provider system: https://a[redacted]

Signing Key

```
{
  "keys": [
    {
      "kty": "RSA",
      "e": "AQAB",
      "use": "sig",
      "kid":
```

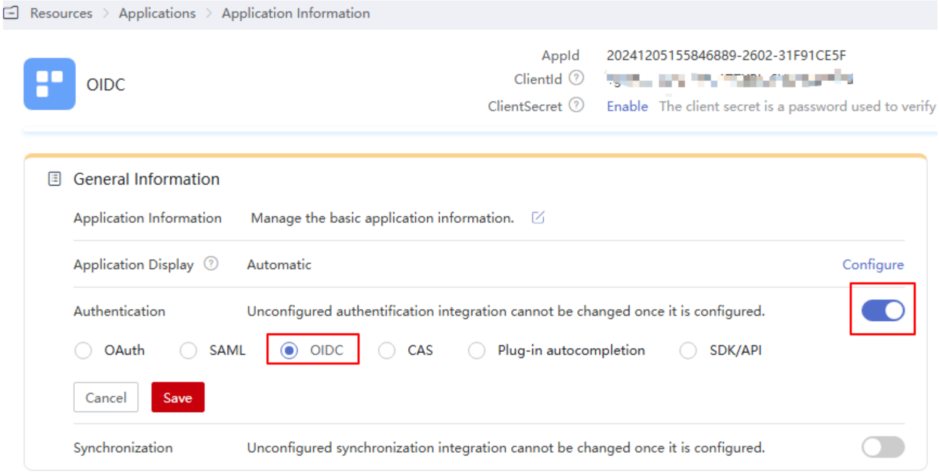
Step 3 Configure identity conversion rules on Huawei Cloud so that OneAccess users can access CodeArts. For details, see **Configure Identity Conversion Rules**.

----End

Establishing a Trust Between OneAccess and Huawei Cloud

Configure the login address and redirect URI of Huawei Cloud in OneAccess.

1. Log in to the OneAccess administrator portal, and choose **Resources** > **Applications**.
2. Click the added custom Huawei Cloud application.
3. Enable **Authentication**, select **OIDC**, and click **Save**.



Resources > Applications > Application Information

OIDC

AppId 20241205155846889-2602-31F91CE5F

ClientId [redacted]

ClientSecret Enable The client secret is a password used to verify

General Information

Application Information: Manage the basic application information.

Application Display: Automatic — Configure

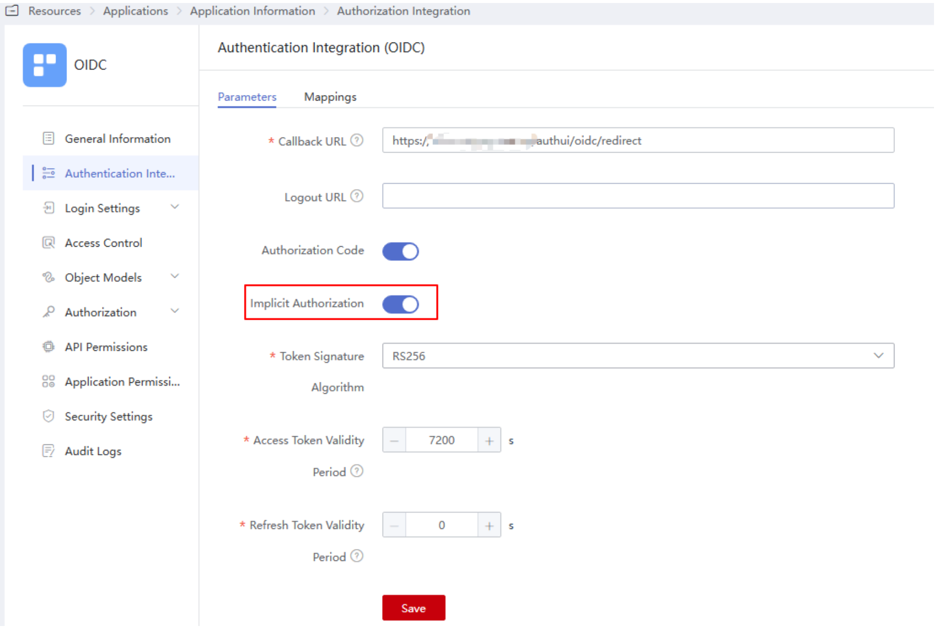
Authentication: Unconfigured authentification integration cannot be changed once it is configured.

○ OAuth ○ SAML ● OIDC ○ CAS ○ Plug-in autocompletion ○ SDK/API

Cancel Save

Synchronization: Unconfigured synchronization integration cannot be changed once it is configured.

4. Click **Configure** on the right of **Authentication**. On the OIDC configuration page displayed, set **Callback URL** to the value of the redirect URI obtained in **Step 2** and enable **Implicit Authorization**.



* Callback URL: https:/[redacted]authui/oidc/redirect

Logout URL:

Authorization Code: ●

Implicit Authorization: ●

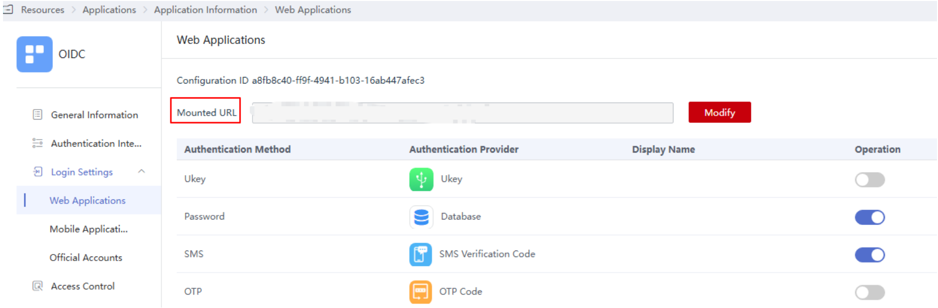
* Token Signature Algorithm: RS256

* Access Token Validity Period: 7200 s

* Refresh Token Validity Period: 0 s

5. Configure the Huawei Cloud login entry in OneAccess.

   On the Huawei Cloud application details page, choose **Login Settings** > **Web Applications**, click **Modify**, replace the URL with the login URL of the IdP created on Huawei Cloud, and click **OK** to save it.



Configuration ID a8fb8c40-ff9f-4941-b103-16ab447afec3

Mounted URL [redacted]

Authentication Method	Authentication Provider	Display Name	Operation
Ukey	Ukey		○
Password	Database		●
SMS	SMS Verification Code		●
OTP	OTP Code		○

NOTE

To redirect to a specific service page on the Huawei Cloud console, combine the login link of the identity provider created on Huawei Cloud and enter the combined URL. The following takes CodeArts as an example:

Login link of the identity provider created on Huawei Cloud: **https://auth.huawei.com/authui/federation/websso?domain_id=e35f***************79ba14839c&idp=one001&protocol=oidc**

CodeArts service address: https://console-intl.huaweicloud.com/devcloud/?locale=en-us#

If the service address contains the **agencyId=***&** field, delete the field, use **&service=** to combine the two addresses, and enter the combined address in the URL.

```
https://auth.huawei.com/authui/federation/websso?
domain_id=e35f94************14839c&idp=SAML-
OneAccess&protocol=saml&service=https://console-intl.huaweicloud.com/devcloud/?
locale=zh-cn#
```

6. Grant Huawei Cloud access permissions to users in OneAccess.

   On the Huawei Cloud application details page, choose **Authorization** > **Application Accounts**, click the button for adding accounts, select required accounts, and click **Save**. The selected accounts can access Huawei Cloud via OneAccess without a password.

NOTE

The email address field of an IAM user is mandatory. Users authorized in OneAccess must have this field.

Logging In as a User

Users with Huawei Cloud access permissions can easily access CodeArts with a single click after logging in to the OneAccess user portal.

3.2 SSO 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 3-1 Terms

Term	Description
IdP	Identity provider (IdP): 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 (SSO): allows users to access a trusted service provider (SP) through a specific redirect URL in OneAccess.

- Authorization process
  a. A user accesses a web application using a browser.
  b. The web application generates a SAML authentication request.
  c. The web application system sends the redirection 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 username of the authenticated user.

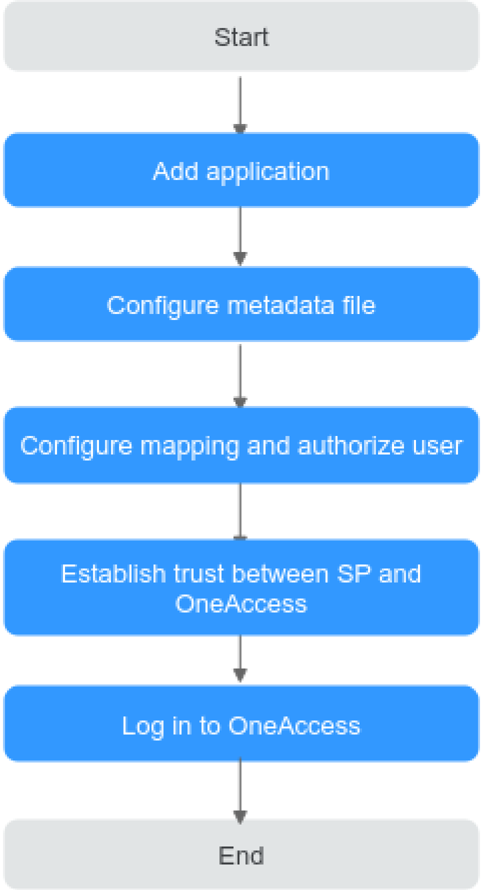
f. The browser forwards the SAML response to the assertion consumer service (ACS) URL of the web application.

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 website.

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.

Configuration Process


Start
Add application
Configure metadata file
Configure mapping and authorize user
Establish trust between SP and OneAccess
Log in to OneAccess
End

Prerequisite

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. Use an existing enterprise account to log in to Huawei Cloud. For details, see **Logging In to the Huawei Cloud Through User Portal**.

Step 1 Log in to the administrator portal.

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

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

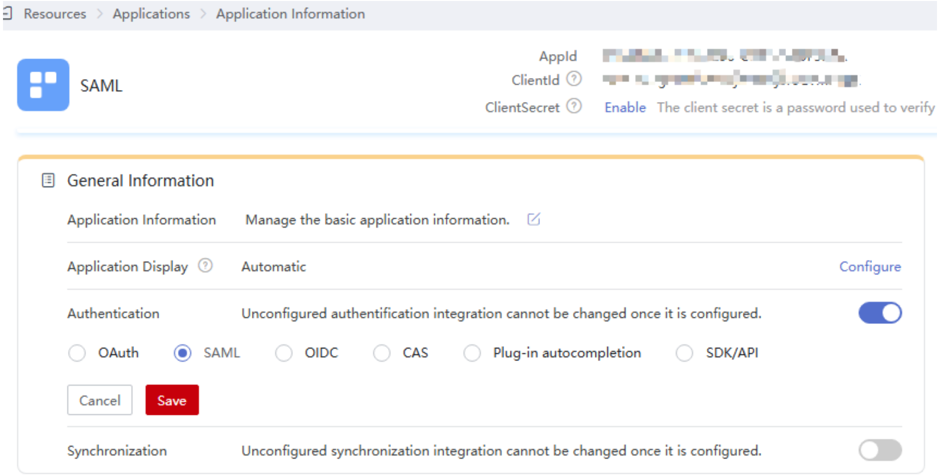
----End

Configuring 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 In the **General Information** area, click next to **Authentication** to enable authentication, select **SAML**, and click **Save**.



Resources > Applications > Application Information

SAML

AppId [redacted]
ClientId [redacted]
ClientSecret Enable The client secret is a password used to verify

General Information

Application Information Manage the basic application information.

Application Display Automatic Configure

Authentication Unconfigured authentification integration cannot be changed once it is configured.

○ OAuth ● SAML ○ OIDC ○ CAS ○ Plug-in autocompletion ○ SDK/API

Cancel Save

Synchronization Unconfigured synchronization integration cannot be changed once it is configured.

NOTE

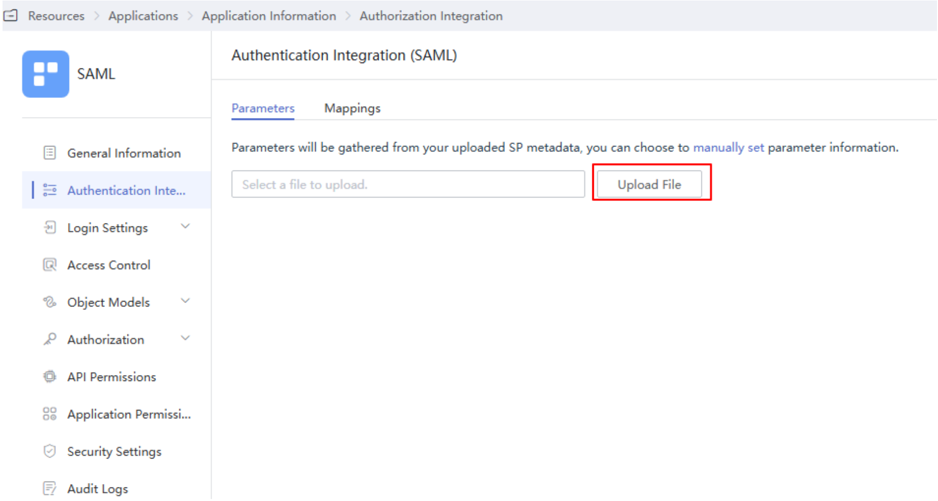
The protocol cannot be changed once specified.

Step 3 In the **General Information** area, click **Configure** next to **Authentication**. On the **Parameters** tab page, configure the metadata file. You can upload a file or configure the parameters.

NOTICE

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

- Uploading a file
   a. Click **Select File** and select the metadata file of the SP.



Parameters will be gathered from your uploaded SP metadata, you can choose to manually set parameter information.

b. If a message displays indicating that the upload is successful, the system has extracted the metadata.

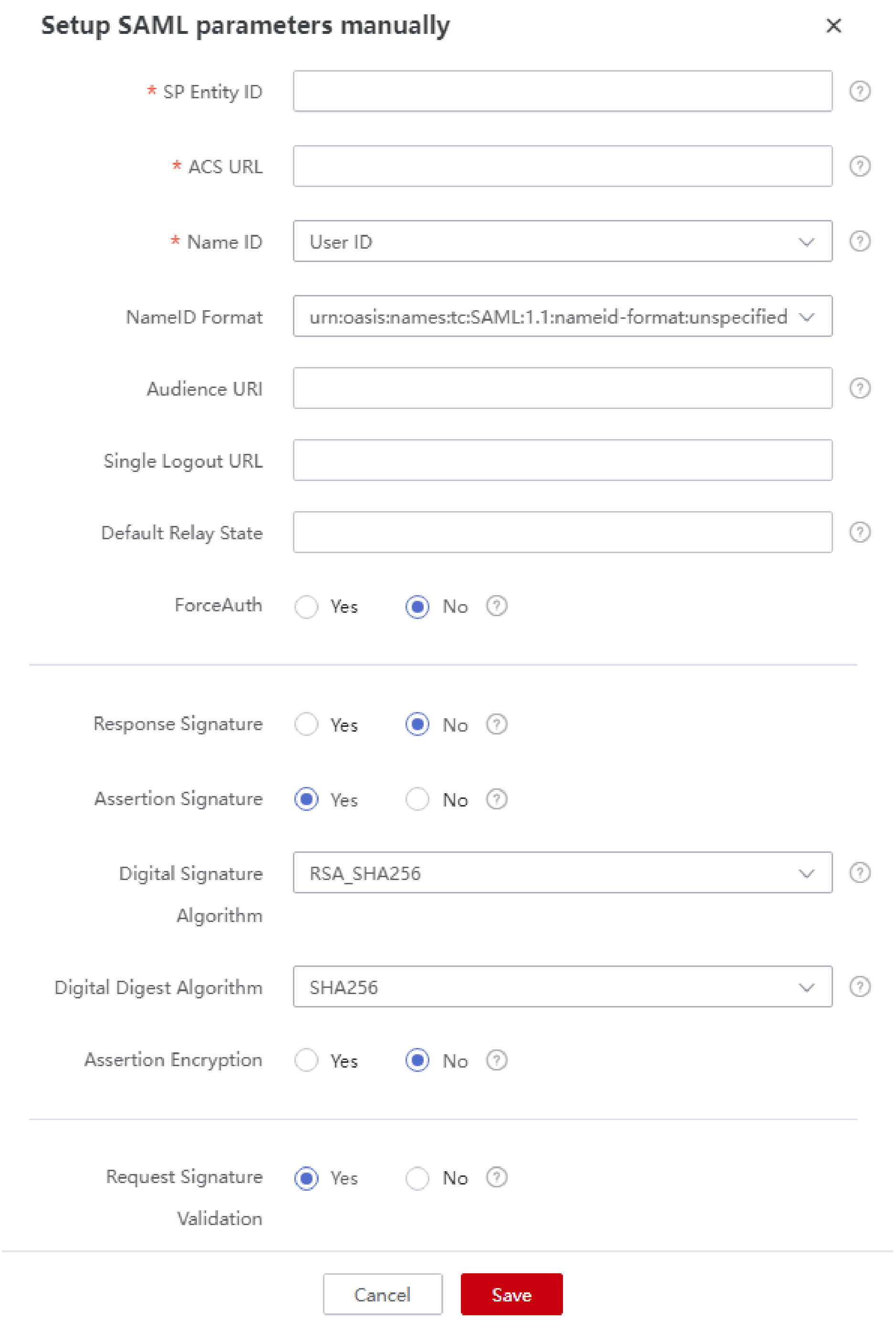
NOTE

- If a message displays indicating that the file format is incorrect and only XML files are supported, check the file format and upload the metadata file again or configure the parameters.
- For details about how to obtain the metadata of the application, see the application's documentation.

- Configuring parameters

a. On the **Parameters** tab page, click **manually set**.

b. Set the required parameters according to the metadata file of the application, and click **Save**.



Setup SAML parameters manually

* SP Entity ID	
* ACS URL	
* Name ID	User ID
NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Audience URI	
Single Logout URL	
Default Relay State	
ForceAuth	○ Yes ● No
Response Signature	○ Yes ● No
Assertion Signature	● Yes ○ No
Digital Signature Algorithm	RSA_SHA256
Digital Digest Algorithm	SHA256
Assertion Encryption	○ Yes ● No
Request Signature Validation	● Yes ○ No

Table 3-2 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.

Parameter	Mandatory	Description
ACS URL	Yes	SP callback URL that receives a response when OneAccess authentication is successful. Enter the value of **AssertionConsumerService** displayed in the SP metadata file.
Name ID	Yes	Select a user attribute or account attribute. The attribute value will be used as the subject of the assertion.
NameID Format	Yes	Username format supported by the SP. Enter the value of **NameIDFormat** displayed in the SP metadata file.
Audience URI	No	Audience for which the SAML assertion is intended. By default, this field is the same as **SP Entity ID**.
Single Logout URL	No	URL to which users will be redirected after logging out of their sessions in OneAccess.
Default Relay State	No	Default value used during IdP-initiated authentication.
ForceAuth	Yes	Default value: **No**. If this option is enabled, users will be authenticated again as required by the SP.
Response Signature	Yes	Default value: **No**. This option indicates whether to sign SAML responses using the IdP's certificate.
Assertion Signature	Yes	Enabled by default. Assertion requires the IdP's signing certificate. Enter the WantAssertionsSigned value 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	Default value: **No**. 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.

Parameter	Mandatory	Description
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.

----End

Configuring Mappings and Authorizing Users

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

  NOTE

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

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

  Table 3-3 Mapping parameters

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

- Then authorize specific users to access the application.

  In the left pane, choose **Authorization** > **Application Accounts**. Then click the button for adding 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 **Configuring an Application**.

  NOTE

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

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** > **Service Settings**.
3. Click **IDP**.
4. On the IdP configuration 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.

3.3 SSO Access to Applications Through OAuth 2.0

Introduction

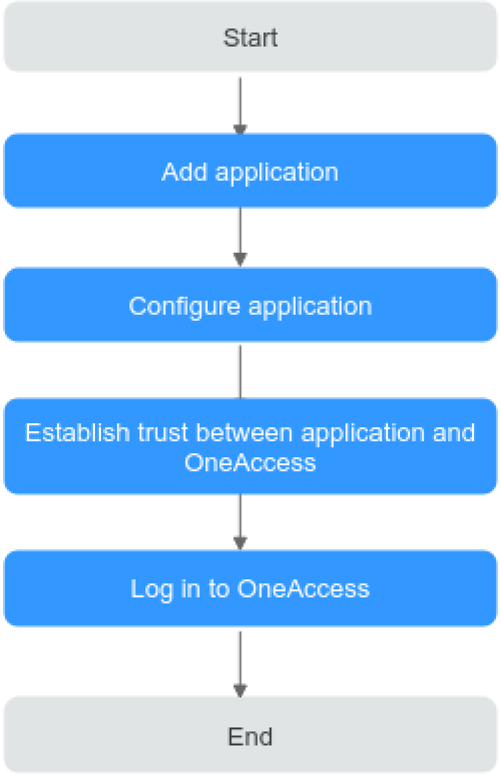
OAuth 2.0 is an open standard that allows users to authorize third-party applications to access their information stored on a specific resource server without sharing usernames and passwords with the third-party applications.

The overall authorization process is as follows:

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.
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



Prerequisite

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 On the top navigation bar, 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

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

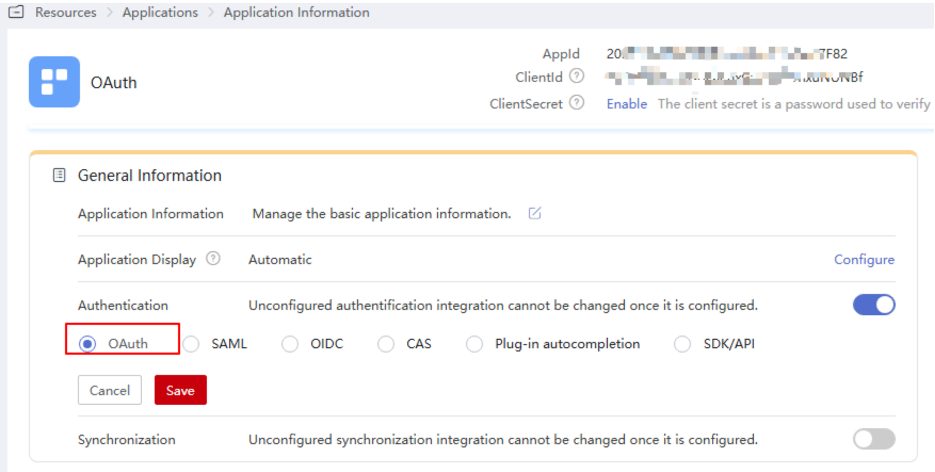
- Authentication configuration
  a. Click the application added in **Adding an Application** and click the application icon on the application information page.

b. In the **General Information** area, click next to **Authentication** to enable authentication, select **OAuth**, and click **Save**.

NOTE

The protocol cannot be changed once specified.

Figure 3-3 Selecting an authentication protocol



AppId 20[redacted]7F82
ClientId [redacted]
ClientSecret Enable The client secret is a password used to verify

Application Information Manage the basic application information.

Application Display Automatic

Authentication Unconfigured authentification integration cannot be changed once it is configured.

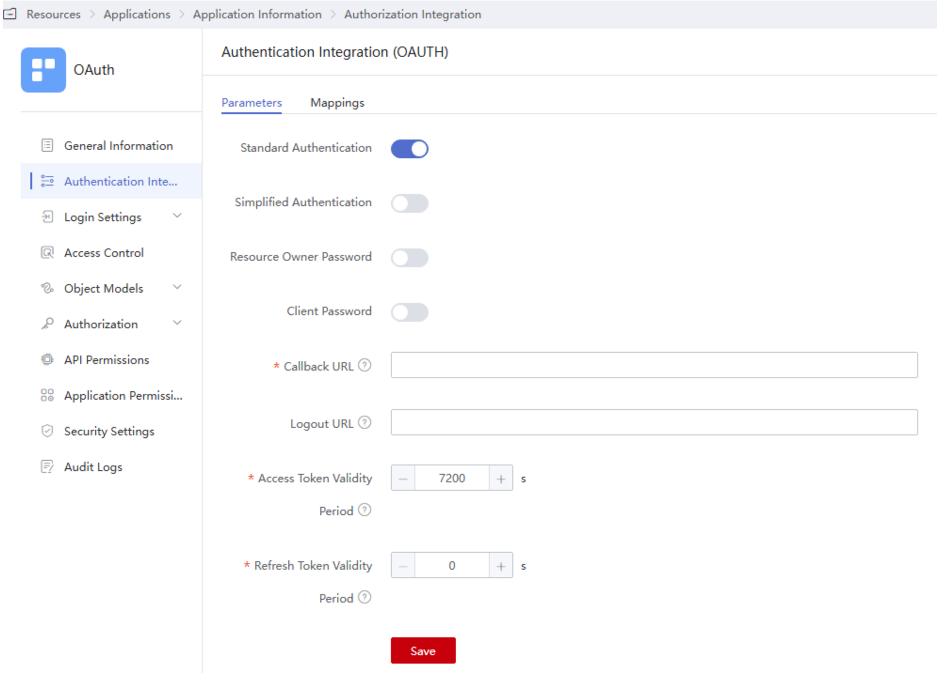
● OAuth ○ SAML ○ OIDC ○ CAS ○ Plug-in autocompletion ○ SDK/API

Synchronization Unconfigured synchronization integration cannot be changed once it is configured.

c. In the **General Information** area, click **Configure** next to **Authentication** to access the OAuth configuration page.

NOTE

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



Standard Authentication: on
Simplified Authentication: off
Resource Owner Password: off
Client Password: off
* Callback URL
Logout URL
* Access Token Validity Period 7200 s
* Refresh Token Validity Period 0 s

Table 3-4 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.
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	Mandatory. (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 home page is recommended, for example, **https://example.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 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

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

Table 3-5 Mapping parameters

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

- Authorizing users

  In the left pane, choose **Authorization** > **Application Accounts**. Then click the button for adding 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 **Configuring an Application**.

  NOTE

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

Establishing a Trust Between the Application and OneAccess

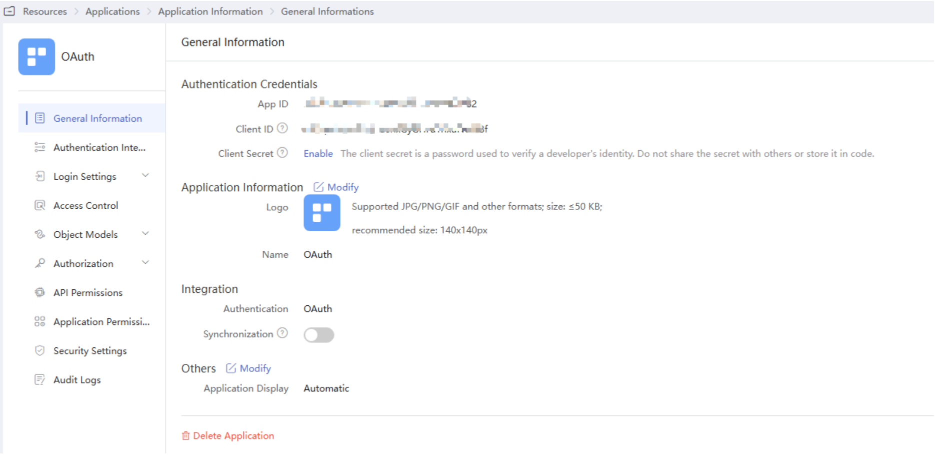
Configure authorization information for OneAccess in the application to establish a trust on OneAccess.

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

- Click **Enable** to generate a client secret.
- Client secret is an important credential used to verify the identity of a developer. Do not provide the client secret to other developers nor store it in code.
- If you reset the client secret, the new client secret takes effect immediately, and all APIs that use the old client secret become invalid. Exercise caution when performing this operation.
- OneAccess does not store the client secret. Keep it properly after obtaining it.



General Information

Authentication Credentials

App ID [redacted]

Client ID [redacted]

Client Secret Enable The client secret is a password used to verify a developer's identity. Do not share the secret with others or store it in code.

Application Information

Logo Supported JPG/PNG/GIF and other formats; size: ≤50 KB; recommended size: 140x140px

Name OAuth

Integration

Authentication OAuth

Synchronization

Others

Application Display Automatic

Step 2 Obtain the authentication information in OneAccess.

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

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.

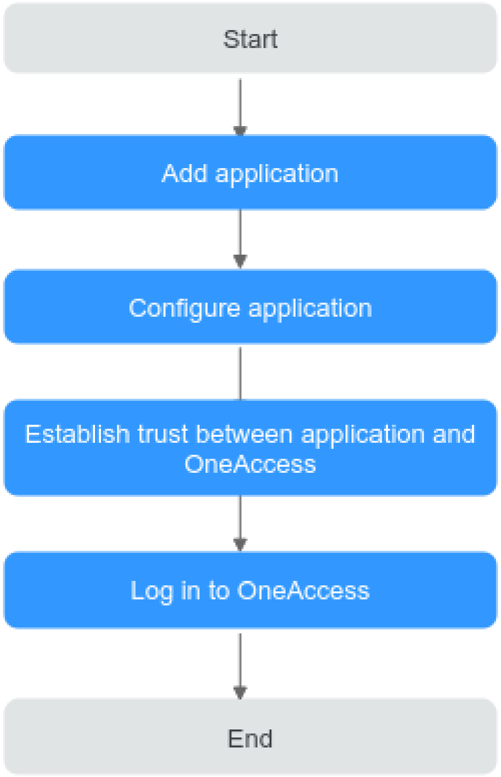
3.4 SSO Access to Applications Through OIDC

Introduction

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

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

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 On the top navigation bar, 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

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

- Authentication configuration

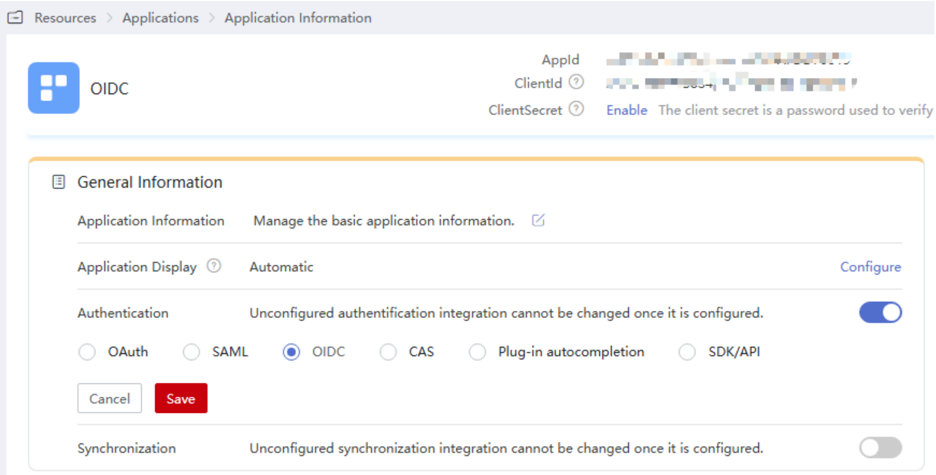
  a. Click the application added in **Adding an Application** and click the application icon on the application information page.

  b. In the **General Information** area, click ○ next to **Authentication** to enable authentication, select **OIDC**, and click **Save**.

  NOTE

  The protocol cannot be changed once specified.

  Figure 3-4 Selecting an authentication protocol



Resources > Applications > Application Information

OIDC

AppId [redacted]
ClientId [redacted]
ClientSecret Enable The client secret is a password used to verify

General Information

Application Information Manage the basic application information.

Application Display Automatic Configure

Authentication Unconfigured authentification integration cannot be changed once it is configured.

○ OAuth ○ SAML ● OIDC ○ CAS ○ Plug-in autocompletion ○ SDK/API

Cancel Save

Synchronization Unconfigured synchronization integration cannot be changed once it is configured.

  c. In the **General Information** area, click **Configure** next to **Authentication** to access the parameter configuration page.

NOTE

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

Table 3-6 Authentication parameters

Parameter	Description
Redirect URL	(Required) Callback URL to be visited after successful authorization. Enter a trusted domain name for receiving and processing authorizations, for example, the domain name of the application home page (**https://xxx.xxx.xxx.com**). Separate domain names using commas (,).
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	Disabled 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. The algorithm should match the encryption algorithm used in the system.
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

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

Table 3-7 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 authorization

  In the left pane, choose **Authorization** > **Application Accounts**. Then click the button for adding 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 **Configuring an Application**.

  NOTE

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

Establishing a Trust Between the Application and OneAccess

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

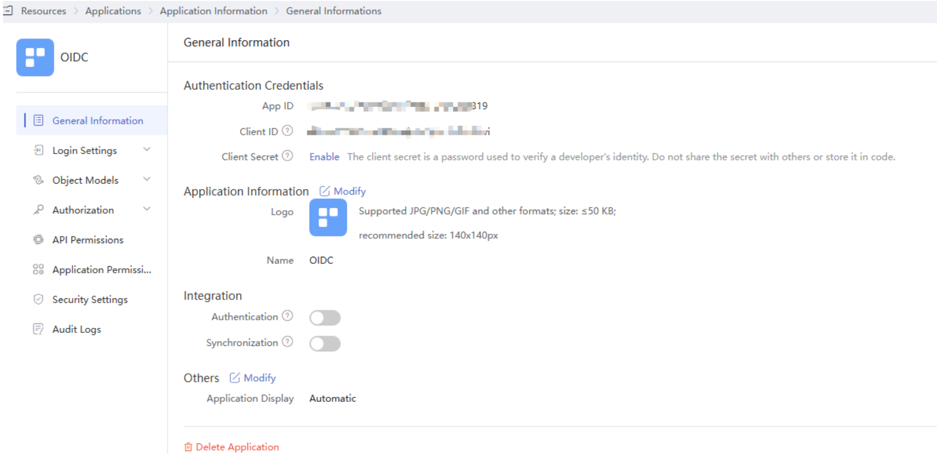
Step 1 Obtain the Client ID and ClientSecret of the application in OneAccess.

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 3-5 Obtaining the Client ID and ClientSecret



General Information

Authentication Credentials

App ID [redacted]

Client ID [redacted]

Client Secret Enable The client secret is a password used to verify a developer's identity. Do not share the secret with others or store it in code.

Application Information

Logo Supported JPG/PNG/GIF and other formats; size: ≤50 KB; recommended size: 140x140px

Name OIDC

Integration

Authentication ○

Synchronization ○

Others

Application Display Automatic

Step 2 Obtain the authentication information in OneAccess.

1. Log in to the administrator portal.
2. In the top navigation pane, choose **Settings** > **Service Settings**.
3. Click **OIDC**.
4. On the OIDC page displayed, check the authentication address, and click **OIDC Settings** in the upper right to check 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.

3.5 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 parts: CAS server and CAS client. They exchange information through the browser. For example, the CAS client can return a redirection message with parameters and forward the message to the CAS server. After the login authentication is successful, the CAS server returns an XML message containing user information to the CAS client. After verifying the user information, the CAS client returns the information to the user for resource access.

  - 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.

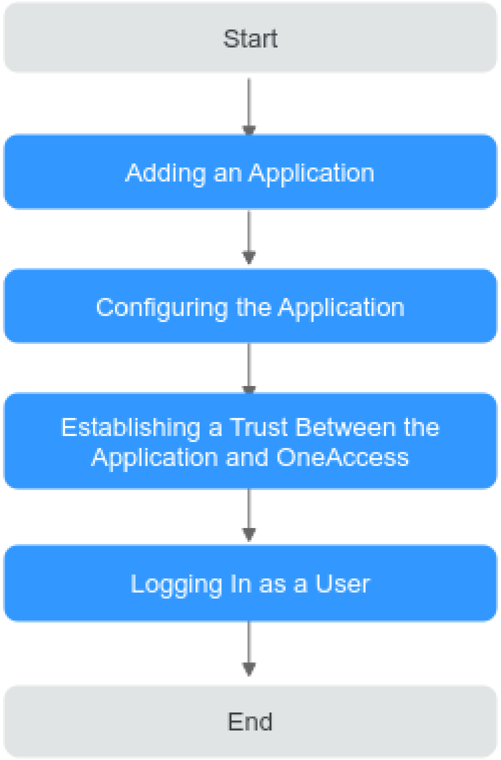
d. After receiving the Service and ST, the CAS client interacts with the CAS server in the background.

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


Start
Adding an Application
Configuring the Application
Establishing a Trust Between the Application and OneAccess
Logging In as a User
End

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 On the top navigation bar, 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

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

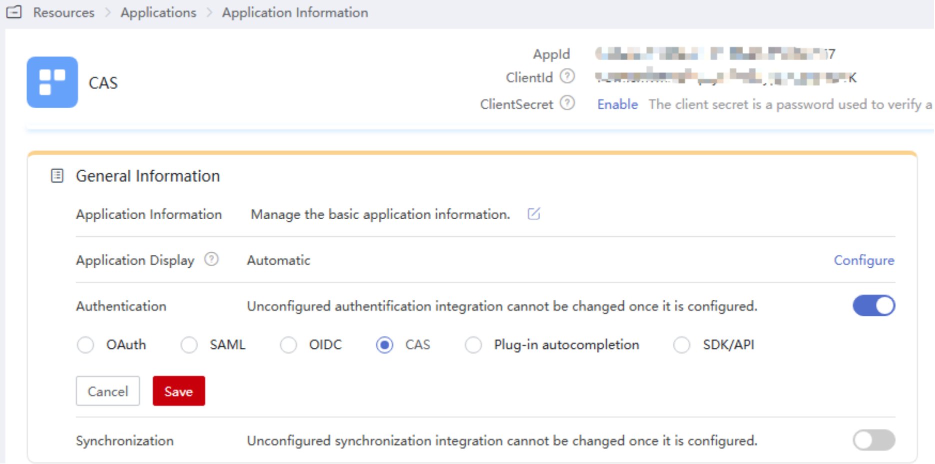
- Authentication configuration
  a. Click the application added in **Adding an Application** and click the application icon on the application information page.

  b. In the **General Information** area, click next to **Authentication** to enable authentication, select **CAS**, and click **Save**.

  NOTE

  The protocol cannot be changed once specified.

  Figure 3-6 Selecting an authentication protocol



Resources > Applications > Application Information

CAS

AppId [redacted]
ClientId ⓘ [redacted]
ClientSecret ⓘ Enable The client secret is a password used to verify a

General Information

Application Information Manage the basic application information.

Application Display ⓘ Automatic Configure

Authentication Unconfigured authentification integration cannot be changed once it is configured.

○ OAuth ○ SAML ○ OIDC ● CAS ○ Plug-in autocompletion ○ SDK/API

Cancel Save

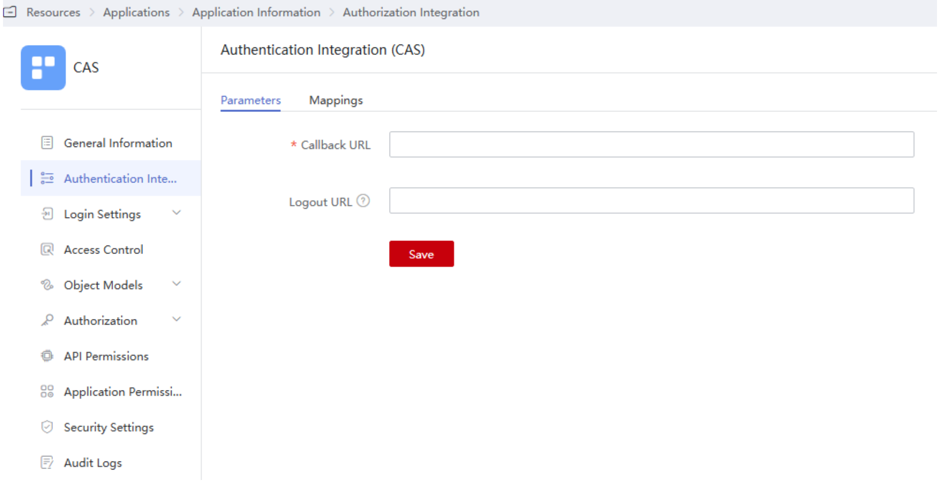
Synchronization Unconfigured synchronization integration cannot be changed once it is configured.

  c. In the **General Information** area, click **Configure** next to **Authentication** to access the CAS configuration page.

NOTICE

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

Figure 3-7 Configuring authentication parameters



Authentication Integration (CAS)

* Callback URL

Logout URL

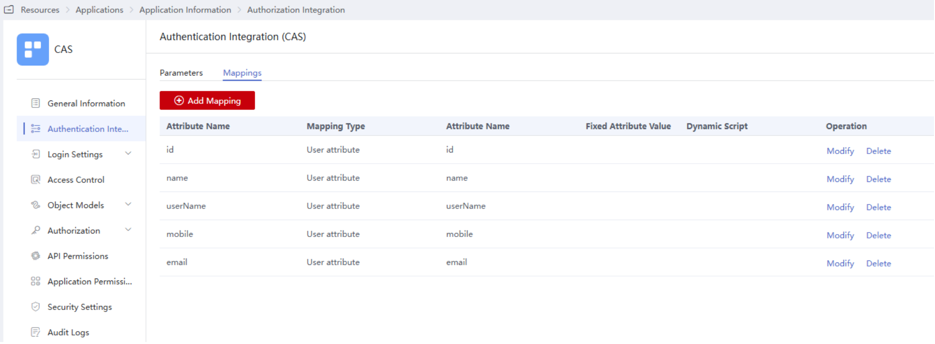
Table 3-8 Authentication parameters

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

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

Figure 3-8 Adding a mapping



Authentication Integration (CAS)

Attribute Name	Mapping Type	Attribute Name	Fixed Attribute Value	Dynamic Script	Operation
id	User attribute	id			Modify Delete
name	User attribute	name			Modify Delete
userName	User attribute	userName			Modify Delete
mobile	User attribute	mobile			Modify Delete
email	User attribute	email			Modify Delete

Table 3-9 Mapping parameters

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

Parameter	Description
Mapping Type	(Required) The mapping type determines the returned attribute value.

- User authorization

  In the left pane, choose **Authorization** > **Application Accounts**. Then click the button for adding 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 **Configuring an Application**.

  NOTE

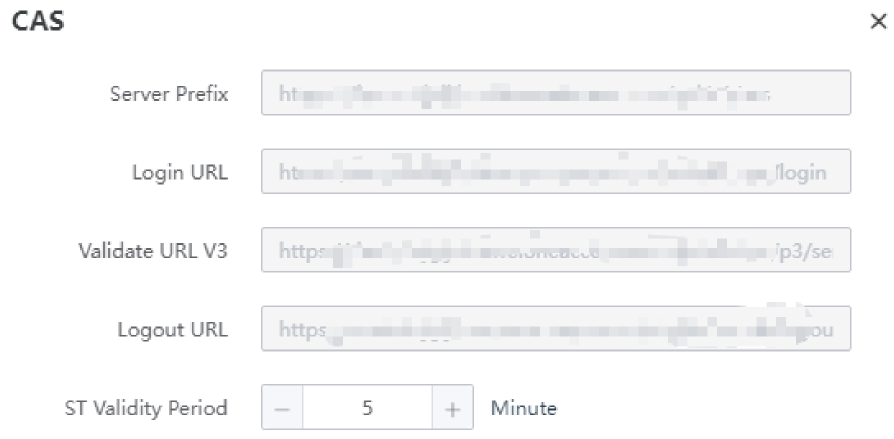
  For details about how to configure login, access control, and object models, see **Configuring an Application**.

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** > **Service Settings**.
3. Click **CAS**.
4. On the **CAS** page, view the authentication address.



CAS

Server Prefix [redacted]

Login URL [redacted]

Validate URL V3 [redacted]

Logout URL [redacted]

ST Validity Period 5 Minute

Table 3-10 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.

Parameter	Description
Validate URL V3	The value is generated by the system and cannot be modified. URL for verifying tickets. V3 URL is recommended.
Logout URL	The value is generated by the system and cannot be modified. URL for logging out of the CAS service.
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

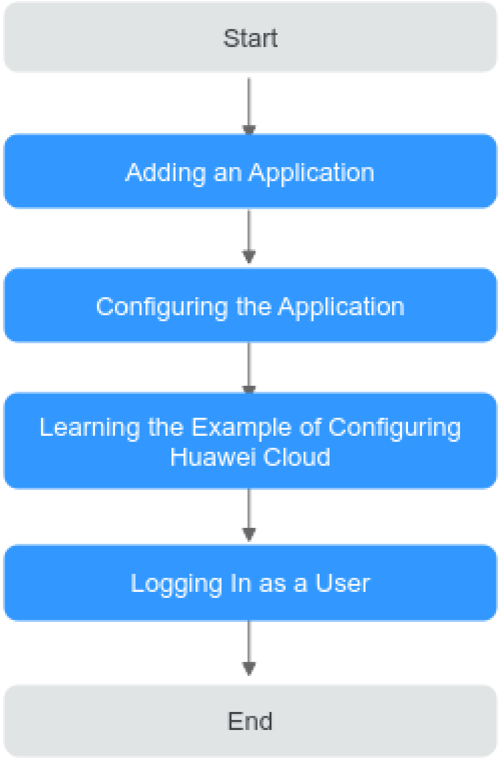
Log in to the user portal as one of the **authorized users**, and click the target application to check whether you can access it.

3.6 SSO Access to Applications Through Plug-in Autocompletion

OneAccess can integrate applications that do not support standard protocols (including OAuth 2.0, SAML, OpenID Connect, and CAS) and cannot be reconstructed on a PC.

This section describes how to integrate an application with OneAccess through plug-in autocompletion.

Configuration Process


Start
Adding an Application
Configuring the Application
Learning the Example of Configuring Huawei Cloud
Logging In as a User
End

Prerequisites

You have permissions to access the administrator portal.

Adding an Application

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, 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

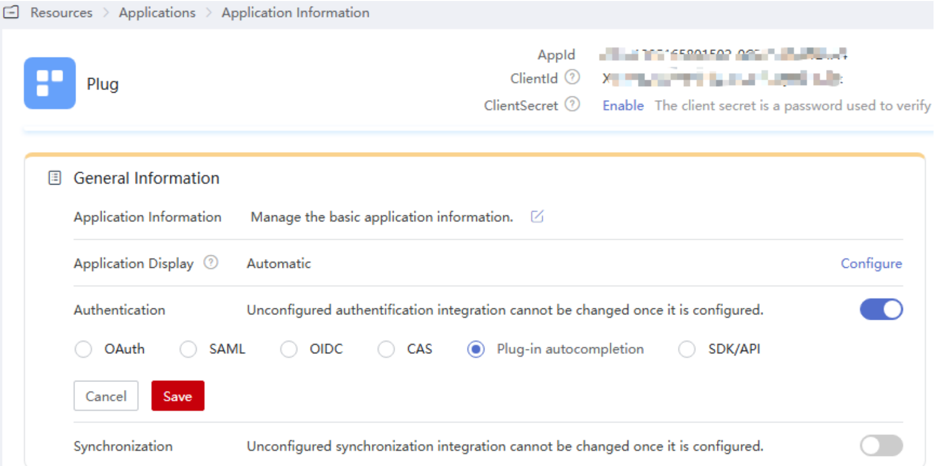
Application configuration includes authentication configuration and user authorization.

- Authentication configuration
  a. Click the application added in **Adding an Application** and click the application icon on the application information page.
  b. In the **General Information** area, click ○ next to **Authentication** to enable authentication, select **Plug-in autocompletion**, and click **Save**.

NOTE

The authentication mode is a one-time configuration and cannot be changed later.

Figure 3-9 Selecting an authentication protocol



Resources > Applications > Application Information

Plug

AppId [redacted]
ClientId [redacted]
ClientSecret Enable The client secret is a password used to verify

General Information

Application Information Manage the basic application information.

Application Display Automatic Configure

Authentication Unconfigured authentification integration cannot be changed once it is configured.

○ OAuth ○ SAML ○ OIDC ○ CAS ● Plug-in autocompletion ○ SDK/API

Cancel Save

Synchronization Unconfigured synchronization integration cannot be changed once it is configured.

c. Click **Authentication Settings** in the left pane, and configure the authentication parameters. OneAccess supports multiple login modes, including quick login, 3-factor login, frame login, and two-page login. The parameters to configure vary depending on the login mode.

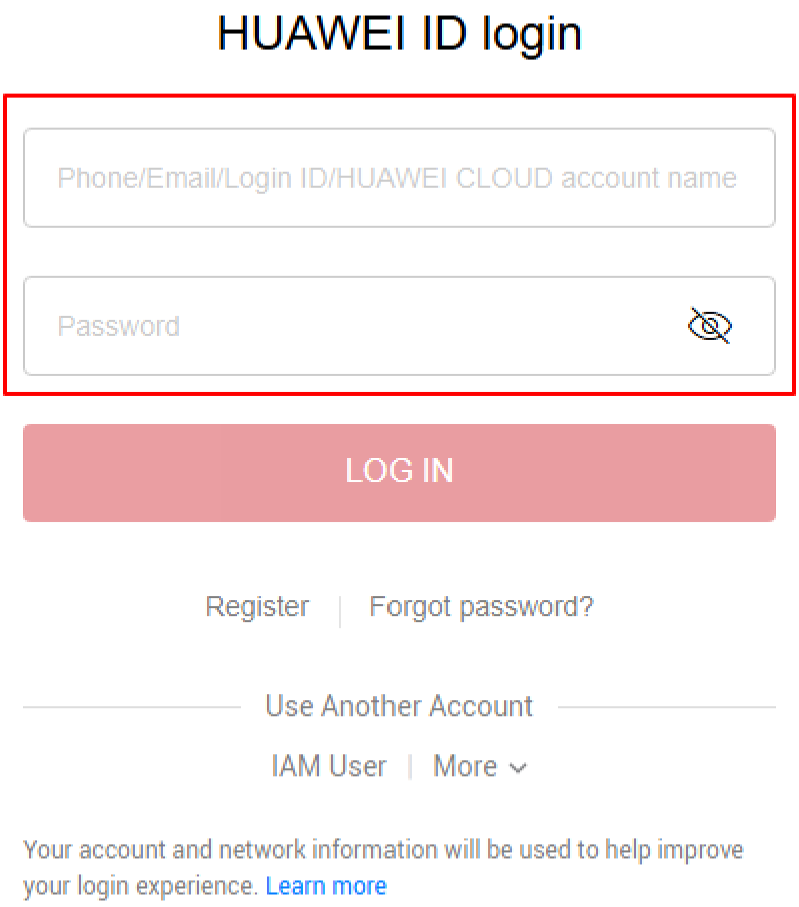
NOTICE

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

- Quick login

  The login page contains only two factors, username and password. Users can log in to the application without entering other information. See **Figure 3-10**.

Figure 3-10 Logging in using a Huawei Cloud account


HUAWEI ID login

Phone/Email/Login ID/HUAWEI CLOUD account name

Password

Your account and network information will be used to help improve your login experience. Learn more

- 3-factor login

  In addition to the username and password, users need to enter other information in a text box or select an option from the drop-down list on the login page. For example, to log in to an internal system, an employee needs to enter their username and password and select their department.

- Frame login

  The username and password fields are enclosed in a frame, which is isolated from the login page.

- Two-page login

  The login process is divided into two pages. To complete login, users need to switch from the first page to the second page.

- 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 **Configuring an Application**.

NOTE

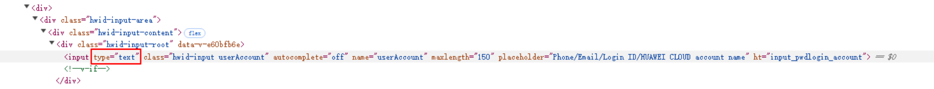
- For details about access control and object models, see **Configuring an Application**.
- User authorization is not required for applications through plug-in autocompletion. Users can directly set the authorization on the user portal.

Example of Configuring Huawei Cloud

The following uses Huawei Cloud as an example to describe how to configure quick login.

Step 1 On the **Huawei Cloud** account login page, press **F12**, locate the account name/email address text box, and obtain the attribute type.

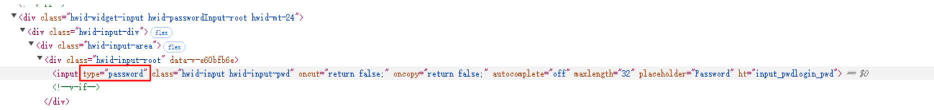
Figure 3-11 Locating the account text box



```
▼<div>
  ▼<div class="hwid-input-area">
    ▼<div class="hwid-input-content"> flex
      ▼<div class="hwid-input-root" data-v-e60bfb6e>
          <input type="text" class="hwid-input userAccount" autocomplete="off" name="userAccount" maxlength="150" placeholder="Phone/Email/Login ID/HUAWEI CLOUD account name" ht="input_pwdlogin_account"> == $0
          <!--v-if-->
        </div>
```

Step 2 Locate the password text box and obtain the attribute type.

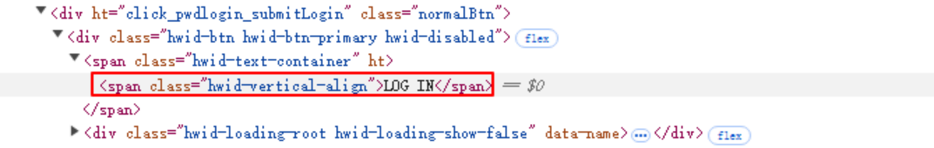
Figure 3-12 Locating the password text box



```
▼<div class="hwid-widget-input hwid-passwordInput-root hwid-mt-24">
  ▼<div class="hwid-input-div"> flex
    ▼<div class="hwid-input-area"> flex
      ▼<div class="hwid-input-root" data-v-e60bfb6e>
          <input type="password" class="hwid-input hwid-input-pwd" oncut="return false;" oncopy="return false;" autocomplete="off" maxlength="32" placeholder="Password" ht="input_pwdlogin_pwd"> == $0
          <!--v-if-->
        </div>
```

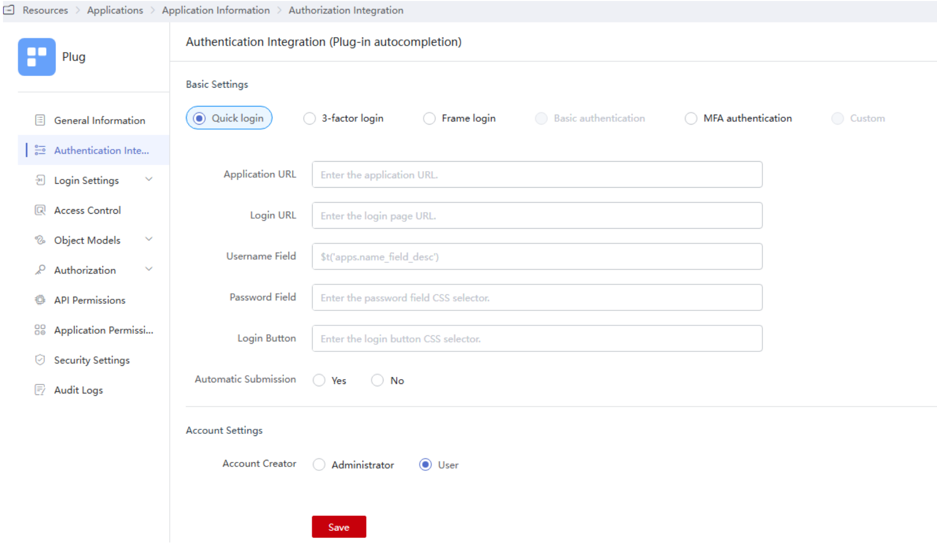
Step 3 Locate the login button and obtain the attribute ID.

Figure 3-13 Locating the login button



```
▼<div ht="click_pwdlogin_submitLogin" class="normalBtn">
  ▼<div class="hwid-btn hwid-btn-primary hwid-disabled"> flex
    ▼<span class="hwid-text-container" ht>
        <span class="hwid-vertical-align">LOG IN</span> == $0
      </span>
    ▶<div class="hwid-loading-root hwid-loading-show-false" data-name>…</div> flex
```

Step 4 Configure the parameters for quick login.



Authentication Integration (Plug-in autocompletion)

Basic Settings

● Quick login ○ 3-factor login ○ Frame login ○ Basic authentication ○ MFA authentication ○ Custom

Application URL: Enter the application URL.

Login URL: Enter the login page URL.

Username Field: $t('apps.name_field_desc')

Password Field: Enter the password field CSS selector.

Login Button: Enter the login button CSS selector.

Automatic Submission: ○ Yes ○ No

Account Settings

Account Creator: ○ Administrator ● User

Table 3-11 Basic settings

Parameter	Description
Application URL	Access URL of the application. You are advised to set this parameter to the home page of the application.
Login URL	Login page URL of the application. This parameter is required when you configure quick login, 3-factor login, or two-page login.
Frame URL	Frame address of the application. This parameter is required when you configure frame login.
Username Field	CSS selector for the username text box.
Next Button	CSS selector for the **Next** button. This parameter is required when you configure two-page login.
Password Field	CSS selector for the password text box.
Extra Field	CSS selector for an additional text box. This parameter is required when you configure 3-factor login.
Extra Mapping Field	Mapping attribute of an additional field. You can select the account name, full name, or password. This parameter is required when you configure 3-factor login.
Login Button	CSS selector for the **Log In** button.
Automatic Submission	Indicates whether the form (username and password) needs to be submitted automatically. If you select **No**, the form will be not be submitted automatically after a user enters their username and password. **NOTE** If human-machine verification is involved on the login page, you are advised to select **No**.

Table 3-12 Account settings

Parameter	Description
Account Creator	Owner of the account used to log in to the application. The options include **Administrator** and **User**. **NOTE** If **Account Creator** is set to **Administrator**, you need to set **Attributes to Set**. If you select **Password**, only users can set their password for logging in to the application.

----End

Logging In as a User

Step 1 Log in to the user portal as an **authorized user**, and download the plug-in as prompted after successful login.

Step 2 Decompress the plug-in package, drag the plug-in to **Extensions**, and then enable it.

Step 3 Refresh the page of user portal and click the target application. A dialog box is displayed, asking you to enter the password. Enter the password and click the login button.

NOTE

If the **Attributes to Set** parameter in **Step 4** is set to **Password**, only the password can be set in this step.

----End

4 Data Synchronization

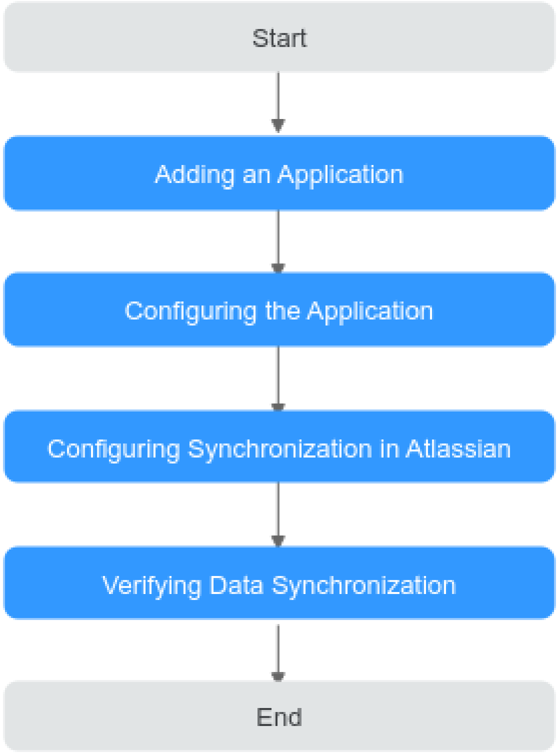
4.1 Synchronizing Data to Atlassian Through SCIM

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.

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

Configuration Process


Start
Adding an Application
Configuring the Application
Configuring Synchronization in Atlassian
Verifying Data Synchronization
End

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 On the top navigation bar, 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**.

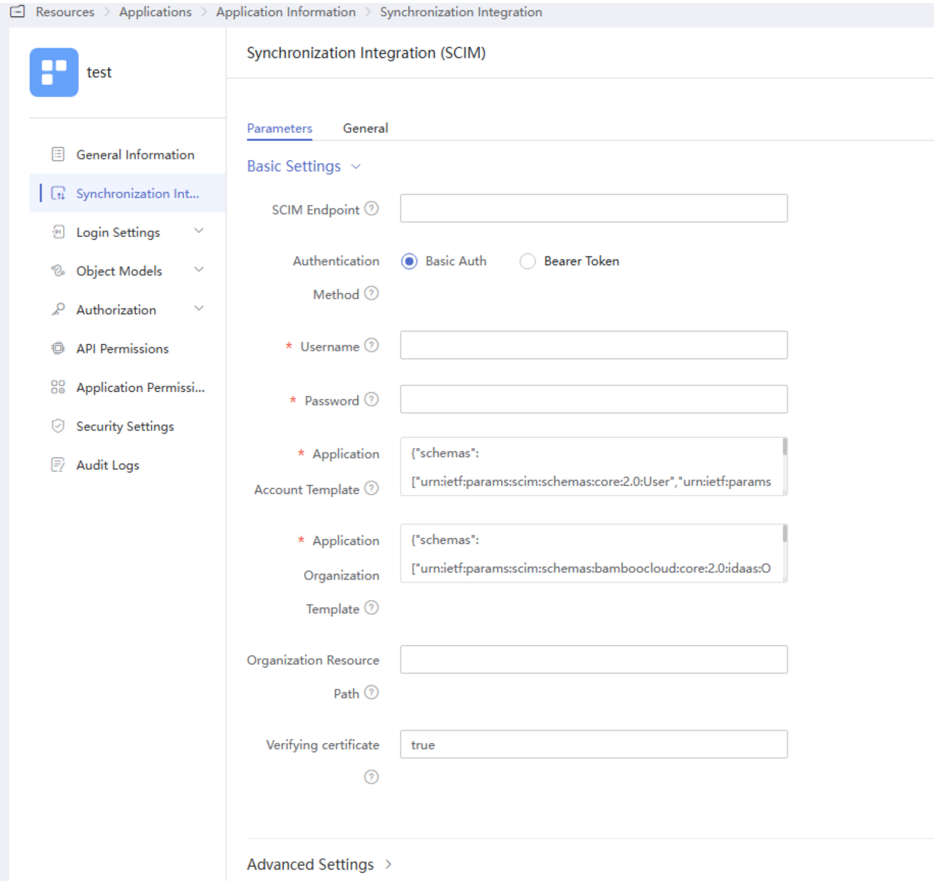
Step 2 In the **General Information** area, click next to **Synchronization** to enable synchronization, select **SCIM**, and click **Save**.

NOTE

The protocol cannot be changed once specified.

Step 3 In the **General Information** area, click **Configure** next to **Synchronization** to access the configuration page.

Figure 4-1 Configuring synchronization parameters



Synchronization Integration (SCIM)

SCIM Endpoint

Authentication Method: ● Basic Auth ○ Bearer Token

* Username

* Password

* Application Account Template: {"schemas": ["urn:ietf:params:scim:schemas:core:2.0:User","urn:ietf:params

* Application Organization Template: {"schemas": ["urn:ietf:params:scim:schemas:bamboocloud:core:2.0:idaas:O

Organization Resource Path

Verifying certificate: true

Table 4-1 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	Authorization is required for calling SCIM APIs. The options include **Basic Auth** (default) and **Bearer Token**.
Username	Yes	Username for authentication. Set this parameter if you specify the authentication method as **Basic Auth**.
Password	Yes	Password of the user. Set this parameter if you specify the authentication method as **Basic Auth**.
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.

Parameter	Mandatory	Description
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 4-2 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 Accounts** in the left pane, click the **Attributes** tab, and click **Add** to add attributes. For details, see **Table 4-3**.

NOTE

The email attribute is mandatory for SCIM to synchronize data from Atlassian. If the attribute is not added, the synchronization fails.

Table 4-3 Attributes

Parameter	Description
Attribute	Attribute that OneAccess will map to the target application, for example, **email**.
Label	Identifier of an attribute name. It is recommended that the value of this parameter match that of **Attribute**.
Description	Description of **Attribute**.

Parameter	Description
Attribute Type	Type of an attribute. You can select a value from the drop-down list box.
Format	This parameter specifies the text format. It can be set only when **Attribute Type** is set to **Text**.
Required	If this option is selected, the attribute must be set when user data is synchronized to an application. If the attribute is left blank, a prompt message is displayed.
Unique	It can be set only when **Attribute Type** is set to **Text**. If this option is selected, the attribute value is kept unique when user data is synchronized to an application. If the attribute is duplicate, a prompt message is displayed.
Sensitive	It can be set only when **Attribute Type** is set to **Text**. If this option is selected, the user data is hidden when it is synchronized to an application. You can click 👁 to view the content.

Step 5 Switch to the **Mappings** tab page, click **Modify**, and configure attribute mappings.

Table 4-4 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.
Application Accounts	Account attribute of the application.

Step 6 In the left pane, choose **Authorization** > **Application Accounts**. Then click the button for adding 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 **Configuring an Application**.

NOTE

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

----End

Configuring Synchronization in Atlassian

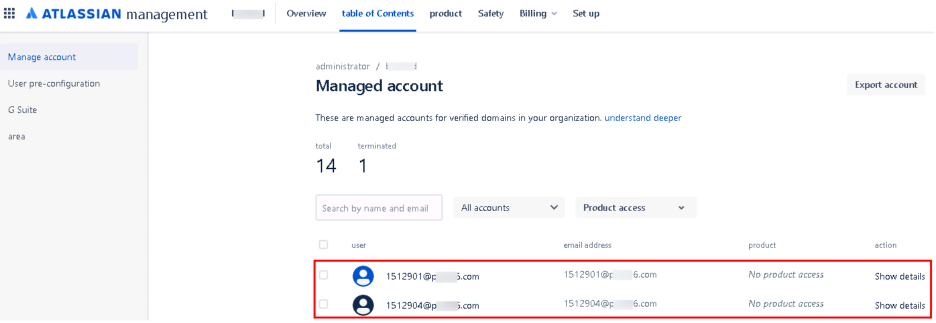
Step 1 Log in to Atlassian.

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.



Managed account

These are managed accounts for verified domains in your organization. understand deeper

total	terminated
14	1

user	email address	product	action
1512901@p[redacted]5.com	1512901@p[redacted]6.com	No product access	Show details
1512904@p[redacted]5.com	1512904@p[redacted]6.com	No product access	Show details

Step 2 Choose **Authorization** > **Synchronization Events** in the left pane, and view the synchronization records.

----End

4.2 Synchronizing Data Through LDAP

LDAP is a 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.

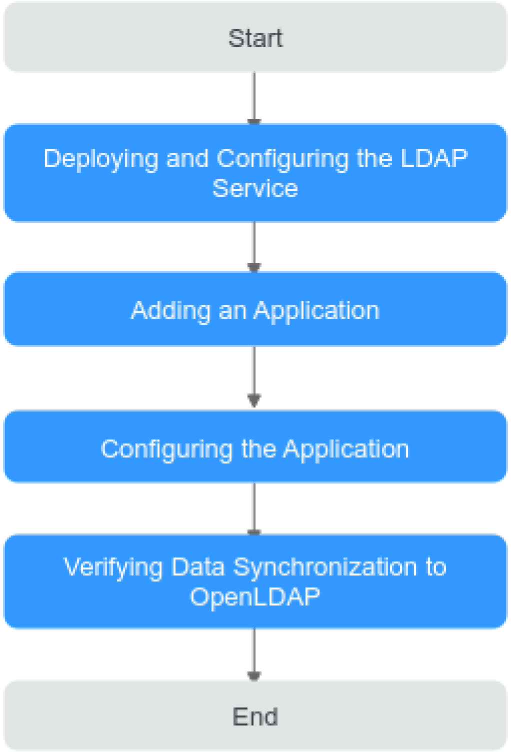
Table 4-5 Terms

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.

Term	Description
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 synchronize organization and user data to OpenLDAP through the LDAP protocol.

Configuration Process


Start
Deploying and Configuring the LDAP Service
Adding an Application
Configuring the Application
Verifying Data Synchronization to OpenLDAP
End

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 On the top navigation bar, 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**.

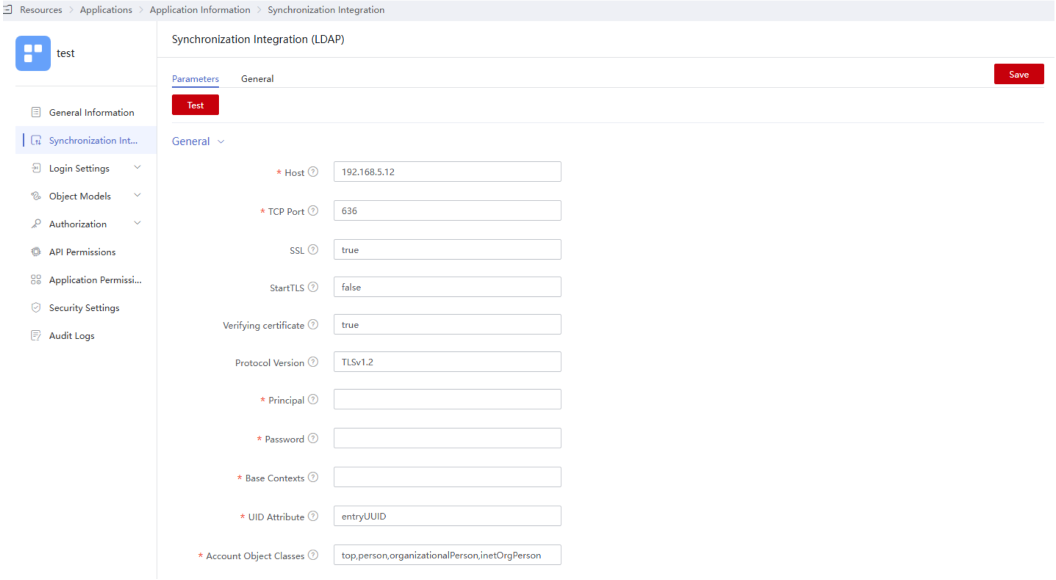
Step 2 In the **General Information** area, click next to **Synchronization** to enable synchronization, select **LDAP**, and click **Save**.

NOTE

The protocol cannot be changed once specified.

Step 3 In the **General Information** area, click **Configure** next to **Synchronization** to access the configuration page.

Figure 4-2 Configuring synchronization parameters



* Host: 192.168.5.12
* TCP Port: 636
SSL: true
StartTLS: false
Verifying certificate: true
Protocol Version: TLSv1.2
* Principal:
* Password:
* Base Contexts:
* UID Attribute: entryUUID
* Account Object Classes: top,person,organizationalPerson,inetOrgPerson

Table 4-6 Common parameters

Parameter	Description
* Host	Host name or IP address of the LDAP server. **NOTE** OneAccess can be accessed only over public networks. Provide the public network address of your LDAP server.
*TCP Port	TCP/IP port of the LDAP server. The default port is **636**.

Parameter	Description
SSL	Default value: **true**, which indicates that SSL is used to connect the LDAP server.
StartTLS	Whether to enable startTLS for encrypted communication. **true**: StartTLS is enabled, and SSL cannot be set to **true**. **false**: StartTLS is not enabled. If data is synchronized to the AD server, either SSL or StartTLS must be enabled.
Verifying certificate	Whether to verify the certificate. This parameter is valid only when SSL or StartTLS is set to **true**. **true**: Verify the certificate. **false**: Do not verify the certificate. The certificate must be authenticated by the public network. Self-signed certificates cannot be used.
Protocol Version	Default value: **TLSv1.2**. Recommended: **TLSv1.3** and **TLSv1.2**.
* Principal	Identifier used for LDAP server authentication, for example, **cn=admin**, **cn=test**, and **cn=com**.
* Password	Password of the principal.
* Base Contexts	Root node in the LDAP directory to be synchronized.
UID Attribute	Name of the LDAP attribute mapped to the UID attribute. Default value: **entryUUID**.
Account Object Classes	One or more object classes to be used when a new user object is created in the LDAP tree. If you enter multiple object classes, each item occupies a line. Do not use commas (,) or semicolons (;) to separate multiple object classes. Some object classes may require you to specify all object classes in the class hierarchy. The default value is **top**, **person**, **organizationalPerson**, or **inetOrgPerson**.

Table 4-7 Optional parameters

Parameter	Description
Domain Name	If a domain name exists, it should be excluded from the reclaimed username. If there are multiple domain names, separate them with commas (,). The default user name excludes the domain name.
Account Username Attributes	Saves one or more attributes of an account user name. During authentication, these attributes are used to search for the LDAP entry of the username to be authenticated. The default value is **uid** and **cn**.

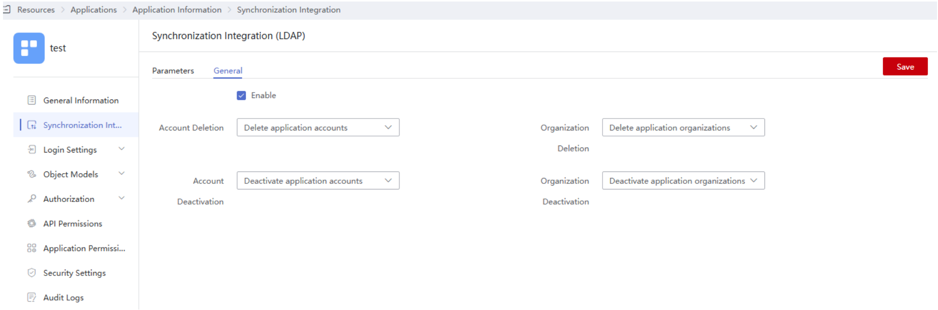
Parameter	Description
Organization Object Classes	One or more object classes to be used when a new organization object is created in the LDAP tree. If you enter multiple object classes, each item occupies a line. Do not use commas (,) or semicolons (;) to separate multiple object classes. Some object classes may require you to specify all object classes in the class hierarchy. The default value is **top** and **organizationalUnit**.
Organization Name Attributes	Stores one or more attributes of the organization name. During authentication, these attributes are used to search for the LDAP entry of the organization name to be authenticated. The default value is **ou**.
Failover Servers	Lists all servers that will be used for failover when the preferred server fails. If the preferred server fails, JNDI will connect to the next available server in the list. Lists all servers in the "**ldap://ldap.example.com:389/**" format (compliant with the standard LDAP v3 URL described in RFC 2255). Only the host and port parts of the URL are relevant in this setting.
Password Attribute	Name of the LDAP attribute used to store passwords. When the password of a user is changed, a new password will be set for this attribute. The default value is **userPassword**. If the password is synchronized to the AD server, set this parameter to **unicodePwd**.
LDAP Filter	Optional LDAP filter used to control the accounts returned from LDAP resources. If no filter is specified, only accounts containing all specified object classes are returned.
Password Hash Algorithm	Algorithm used by the identity system to hash passwords. Currently, **SSHA**, **SHA**, **SMD5**, and **MD5** are supported. A null value indicates that the system does not hash the password. Unless the LDAP server performs hashing (Netscape Directory Server and iPlanet Directory Server perform hashing), this will result in plaintext passwords being stored in LDAP.
Respect Resource Password Policy Change-After-Reset	If this resource is specified in the login module (i.e., this resource is the passing verification target) and the password policy of the resource is configured to change after reset, users who have reset the resource account password for management purpose need to change the password after successful verification. The default value is **false**.
Use VLV Controls	Whether to force the use of VLV controls on standard LDAP controls. The default value is **false**.
VLV Sort Attribute	Sorting attribute used for VLV indexes on resources. Default value: **uid**.

Parameter	Description
Read Schema	If the value is **true**, the connector reads the schema from the server. If **false**, the connector provides a default schema based on the object class in the configuration. To use the extended object class, this attribute must be set to **true**. The default value is **true**.
Base Contexts to Synchronize	One or more starting points in the LDAP tree that are used to determine whether changes should be synchronized. If this attribute is not set, the base context attribute is used to synchronize changes.
Object Classes to Synchronize	Object classes to be synchronized. The change log is for all objects; it filters updates based on the listed object classes. You should not list the superclasses of an object class unless you want to synchronize the object with any superclass value. For example, if only the **inetOrgPerson** object should be synchronized, but the superclasses (**person**, **organizationalperson**, and **top**) of **inetOrgPerson** should be filtered out, only **inetOrgPerson** should be listed here. All objects in LDAP are derived subclasses of **top**. Therefore, **top** should never be listed. Otherwise, no object can be filtered. The default value is **inetOrgPerson**.
Attributes to Synchronize	Name of the attribute to be synchronized. When this option is set, if updates in the change log do not update any named attributes, these updates are ignored. For example, if only **department** is listed, only changes that affect **department** are processed and all other updates are ignored. If you leave it blank (default setting), all changes are processed.
LDAP Filter for Accounts to Synchronize	Optional LDAP filter used for synchronizing objects. Because the change log applies to all objects, this filter updates only the objects that meet the specified filter criteria. If a filter is specified, the object is synchronized only when the object meets the filter conditions and contains the synchronized object class.
Change Log Block Size	Number of change log entries obtained by each query. The default value is **100**.
Change Number Attribute	The name of the change number attribute in the change log entry. The default value is **changeNumber**.
Filter with Or Instead of And	Typically, the filter used to obtain change log entries is to retrieve change entries over a period of time based on the AND condition. If this attribute is set, the filter filters with the OR condition instead with the required number of changes. The default value is **false**.

Parameter	Description
Remove Log Entry Object Class from Filter	If this attribute is set (default), the filter used to obtain change log entries will not contain the **changeLogEntry** object class because the change log should not contain entries of other object classes. The default value is **true**.
Password Attribute to Synchronize	Name of the password attribute to be synchronized during password synchronization.
Status Management Class	Class used to manage the enabling/disabling status. If no class is specified, identity status management cannot be performed.
Retrieve Passwords with Search	Whether to retrieve the user password during search. The default value is **false**.
DN Attribute	DN attribute name of an item. The default value is **entryDN**.
LDAP Filter	Optional LDAP filter that controls the groups returned from LDAP resources. If no filter is specified, only groups containing all specified object classes are returned.
Read Timeout (ms)	Time for waiting for a response. If no response is received within the specified time, the read attempt is aborted. If the value is **0** or less than **0**, there is no limit. The default value is **30000**.
Connection Timeout (ms)	Waiting time for opening a new server connection. The value **0** indicates that the TCP network timeout will be used, which may be several minutes. If the value is less than **0**, there is no limit. The default value is **6000**.
Account DN Prefix	If the value is empty, the default value **cn** is used. You can also set the value to another attribute name used as the DN prefix, such as **uid**.

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

Step 5 Click the **General** tab. On the displayed page, set synchronization data processing logic for **Account Deletion**, **Organization Deletion**, **Account Deactivation**, and **Organization Deactivation**. Then select **Enable** to apply the synchronization data processing logic.



Synchronization Integration (LDAP)

☑ Enable

Account Deletion: Delete application accounts

Organization Deletion: Delete application organizations

Account Deactivation: Deactivate application accounts

Organization Deactivation: Deactivate application organizations

Step 6 To synchronize other user attributes, choose **Object Models** > **Application Accounts** in the left pane, click the **Attributes** tab, and click **Add** to add more attributes. For details, see **Table 4-8**. **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.

Table 4-8 Attributes

Parameter	Description
Attribute	Account attribute of the application system, for example, **employeeNumber**.
Label	Identifier of an attribute name. It is recommended that the value of this parameter match that of **Attribute**.
Description	Description of **Attribute**.
Attribute Type	Type of an attribute. You can select a value from the drop-down list box.
Format	This parameter specifies the text format. It can be set only when **Attribute Type** is set to **Text**.
Required	If this option is selected, the attribute must be set when user data is synchronized to an application. If the attribute is left blank, a prompt message is displayed.
Unique	It can be set only when **Attribute Type** is set to **Text**. If this option is selected, the attribute value is kept unique when user data is synchronized to an application. If the attribute is duplicate, a prompt message is displayed.
Sensitive	It can be set only when **Attribute Type** is set to **Text**. If this option is selected, the user data is hidden when it is synchronized to an application. You can click 👁 to view the content.

Step 7 After you have finished setting the parameters, click **Save**.

Step 8 Switch to the **Mappings** tab page, click **Modify**, and configure attribute mappings.

Table 4-9 Mappings

Parameter	Description
User	Attribute that OneAccess will map to the application, for example, **mobile number**.
Conversion Mode	Attribute mapping mode.
Script Expression	Enter a script if you specify the conversion mode as **Script-based**. For details about mapping scripts, see **Developing Mapping Scripts**.
Execution Mode	Operation to be performed when user data is synchronized from OneAccess to the target application.
Application Accounts	Account attribute of the application.

Step 9 To synchronize organizations, choose **Object Models** > **Application Organization Model**, and click to 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.

Step 10 To synchronize other organization attributes, choose **Object Models** > **Application Organization** in the left pane, click the **Attributes** tab, and click **Add** to add more attributes. For details, see **Table 4-10**.

Table 4-10 Attributes

Parameter	Description
Attribute	Attribute name of an application organization.
Label	Identifier of an attribute name. It is recommended that the value of this parameter match that of **Attribute**.
Description	Description of **Attribute**.
Attribute Type	Type of an attribute. You can select a value from the drop-down list box.
Format	This parameter specifies the text format. It can be set only when **Attribute Type** is set to **Text**.

Parameter	Description
Required	If this option is selected, the attribute must be set when organization data is synchronized to an application. If the attribute is left blank, a prompt message is displayed.
Unique	It can be set only when **Attribute Type** is set to **Text**. If this option is selected, the attribute value is kept unique when organization data is synchronized to an application. If the attribute is duplicate, a prompt message is displayed.
Sensitive	It can be set only when **Attribute Type** is set to **Text**. If this option is selected, the organization data is hidden when it is synchronized to an application. You can click 👁 to view the content.

Step 11 After you have finished setting the parameters, click **Save**.

Step 12 Switch to the **Mappings** tab page, click **Modify**, and configure attribute mappings. For details, see **Table 4-11**.

Table 4-11 Mappings

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**. For details about mapping scripts, see **Developing Mapping Scripts**.
Execution Mode	Operation to be performed when organization data is synchronized from OneAccess to the target application.
Organization	Organization attribute of an application.

----End

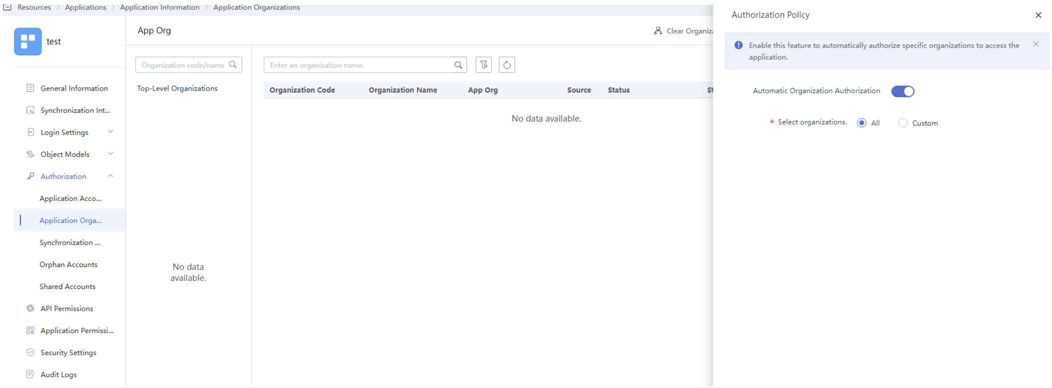
Verifying Data Synchronization to OpenLDAP

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 page.

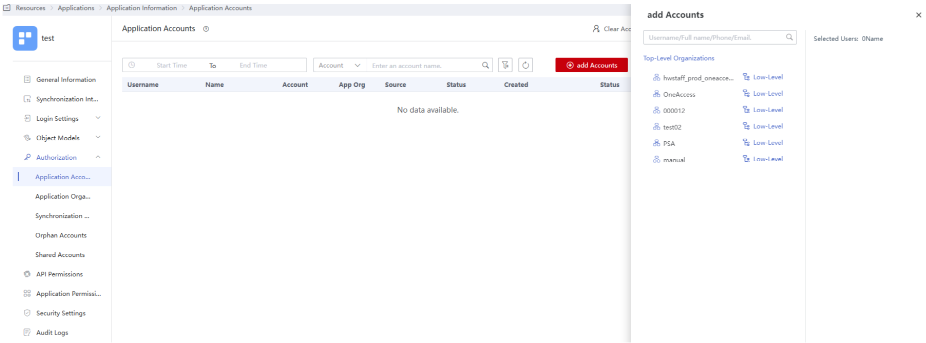
Figure 4-3 Authorizing organizations



Enable this feature to automatically authorize specific organizations to access the application.

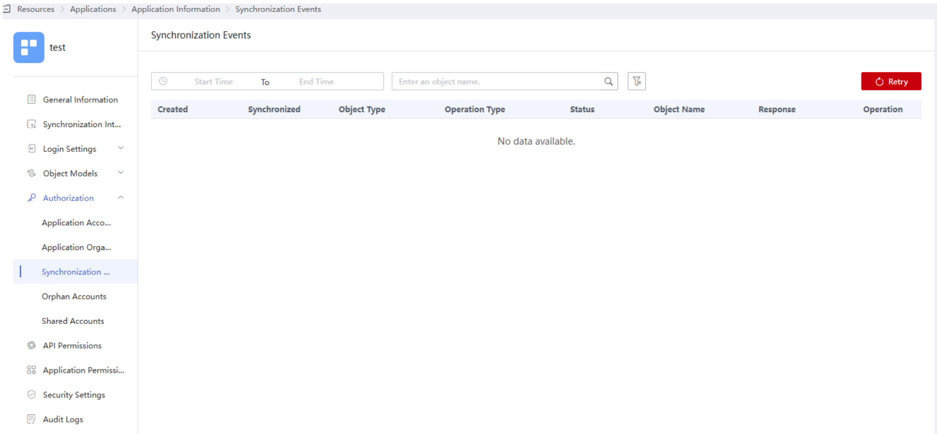
Step 2 In the left pane, choose **Authorization** > **Application Accounts**. Then click **Add Accounts** to authorize specific users to access the application. To authorize access using a policy, see the descriptions about the application account authorization policy in **Configuring an Application**.

Figure 4-4 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.

Figure 4-5 Viewing the synchronization events



Synchronization Events

Created	Synchronized	Object Type	Operation Type	Status	Object Name	Response	Operation

No data available.

Step 4 View the synchronized data in LDAP.

----End

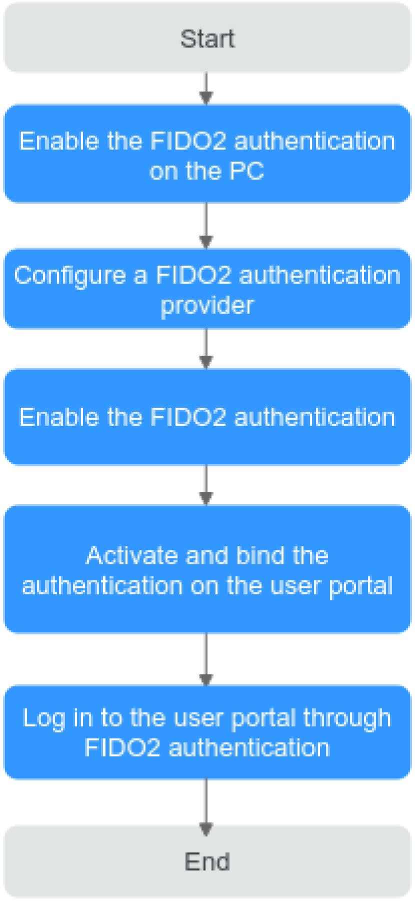
5 Authentication Provider Integration

5.1 Built-in Authentication Providers

Introduction

This section describes how to use the FIDO2 authentication providers (such as facial or fingerprint authentication) to log in to the applications integrated into OneAccess. You can configure the FIDO2 authentication providers on OneAccess and enable the FIDO2 login mode for each application. In this way, SSO is implemented, providing users with more convenient, secure, and reliable login.

Configuration Process


Start
Enable the FIDO2 authentication on the PC
Configure a FIDO2 authentication provider
Enable the FIDO2 authentication
Activate and bind the authentication on the user portal
Log in to the user portal through FIDO2 authentication
End

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.

Prerequisites

- You have permissions to access the administrator portal.
- The user PC uses security keys (USB or Bluetooth) or biometric authenticators (such as Windows Hello and Touch ID).

Enabling FIDO2 Authentication on the PC

Enable the options of security keys (USB or Bluetooth) or biometric authenticators (such as Windows Hello and Touch ID) on the user PC. The following uses Windows Hello as an example.

Configuring a FIDO2 Authentication Provider in OneAccess

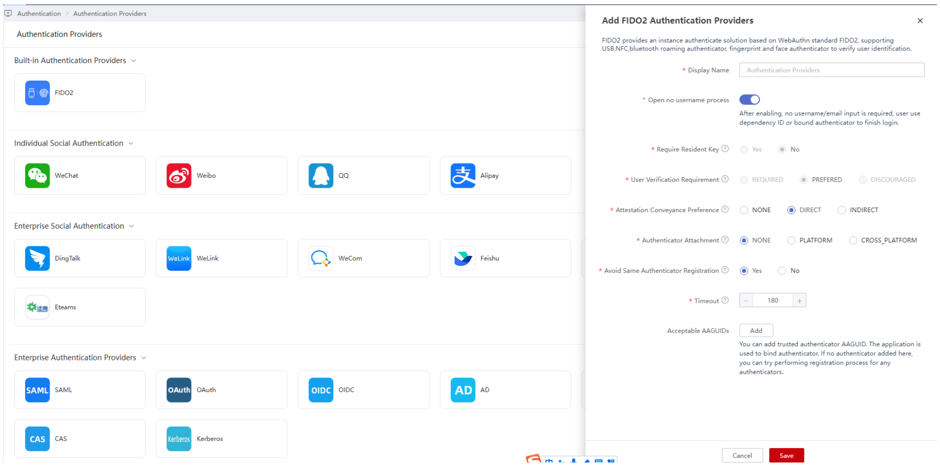
Add a FIDO2 authentication provider and configure the application information in OneAccess.

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, choose **Authentication** > **Authentication Providers**. On the displayed page, choose **Built-in Authentication Providers** > **FIDO2**.

Step 3 Configure authentication provider parameters.

Figure 5-1 Configuring the FIDO2 Authentication provider


Authentication > Authentication Providers
Authentication Providers
Built-in Authentication Providers
FIDO2
Individual Social Authentication
WeChat
Weibo
QQ
Alipay
Enterprise Social Authentication
DingTalk
WeLink
WeCom
Feishu
Eteams
Enterprise Authentication Providers
SAML
OAuth
OIDC
AD
CAS
Kerberos
Cancel
Save

Add FIDO2 Authentication Providers

FIDO2 provides an instance authenticate solution based on WebAuthn standard FIDO2, supporting USB,NFC,bluetooth roaming authenticator, fingerprint and face authenticator to verify user identification.

* Display Name: Authentication Providers

* Open no username process: enabled

After enabling, no username/email input is required, user use dependency ID or bound authenticator to finish login.

* Require Resident Key: ○ Yes ● No

* User Verification Requirement: ○ REQUIRED ● PREFERED ○ DISCOURAGED

* Attestation Conveyance Preference: ○ NONE ● DIRECT ○ INDIRECT

* Authenticator Attachment: ● NONE ○ PLATFORM ○ CROSS_PLATFORM

* Avoid Same Authenticator Registration: ● Yes ○ No

* Timeout: 180

Acceptable AAGUIDs: Add

You can add trusted authenticator AAGUID. The application is used to bind authenticator. If no authenticator added here, you can try performing registration process for any authenticators.

Table 5-1 Configuring parameters

Parameter	Description
Icon	Upload a custom icon.
Display Name	Enter a display name of the authentication provider.
Open no username process	If this function is enabled, users do not need to enter the username or email address for login. Instead, they can select a relying party ID or bound authenticator to find the authenticator private key.
Require Resident Key	Whether to allow the authenticator to produce Public Key Credential as Client-side-resident Public Key Credential Source. Default option: **No**. If you enable login without username, this option will be changed to **Yes**.
User Verification Requirement	Whether to allow the authenticator to confirm the actual authentication user for registration and authentication. Default option: **PREFERRED**. If you enable login without username, this option will be changed to **REQUIRED**.
Attestation Conveyance Preference	Select the preference of the WebAuthn API for generating an attestation. This parameter is used for registration. Default option: **DIRECT**.
Authenticator Attachment	Select an authenticator attachment mode that can be accepted by the WebAuthn client. This parameter is used for registration. Default option: **NONE**.
Avoid Same Authenticator Registration	Whether to allow re-registration of authenticators of the same type. Default option: **Yes**.

Parameter	Description
Timeout	Timeout interval for connecting to the identity authenticator during binding and authentication. Default value: **180**, in seconds.
Acceptable AAGUIDs	(Optional) Add the Authenticator Attestation GUID (AAGUID) of the trusted authenticator. This parameter is used for binding authenticators. If this parameter is left blank, any authenticator can be registered.

----End

Enabling FIDO2 Authentication

Step 1 Log in to the administrator portal.

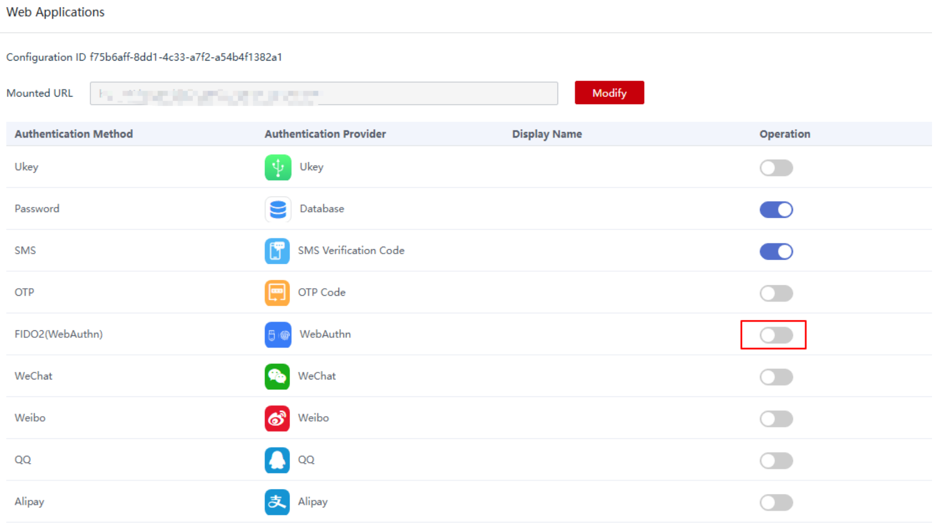
Step 2 On the top navigation bar, choose **Resources** > **Applications**.

Step 3 Click **User Portal** on the page.

Step 4 On the application information page, click the application icon.

Step 5 Choose **Login Settings** > **Web Applications**. In the **Operation** column of the row of **FIDO2(WebAuthn)**, click ○ to enable FIDO2 authentication.

Figure 5-2 Enabling FIDO2 authentication



Web Applications

Configuration ID f75b6aff-8dd1-4c33-a7f2-a54b4f1382a1

Mounted URL [redacted] Modify

Authentication Method	Authentication Provider	Display Name	Operation
Ukey	Ukey		○
Password	Database		●
SMS	SMS Verification Code		●
OTP	OTP Code		○
FIDO2(WebAuthn)	WebAuthn		○
WeChat	WeChat		○
Weibo	Weibo		○
QQ	QQ		○
Alipay	Alipay		○

----End

Activating the Binding on the OneAccess User Portal

Step 1 Log in to the OneAccess user portal, hover the cursor on the username in the upper right corner, and click **Account Settings**.

Step 2 Choose **Account Security** and click the bind button next to the added security key or biometric authenticator.

NOTE

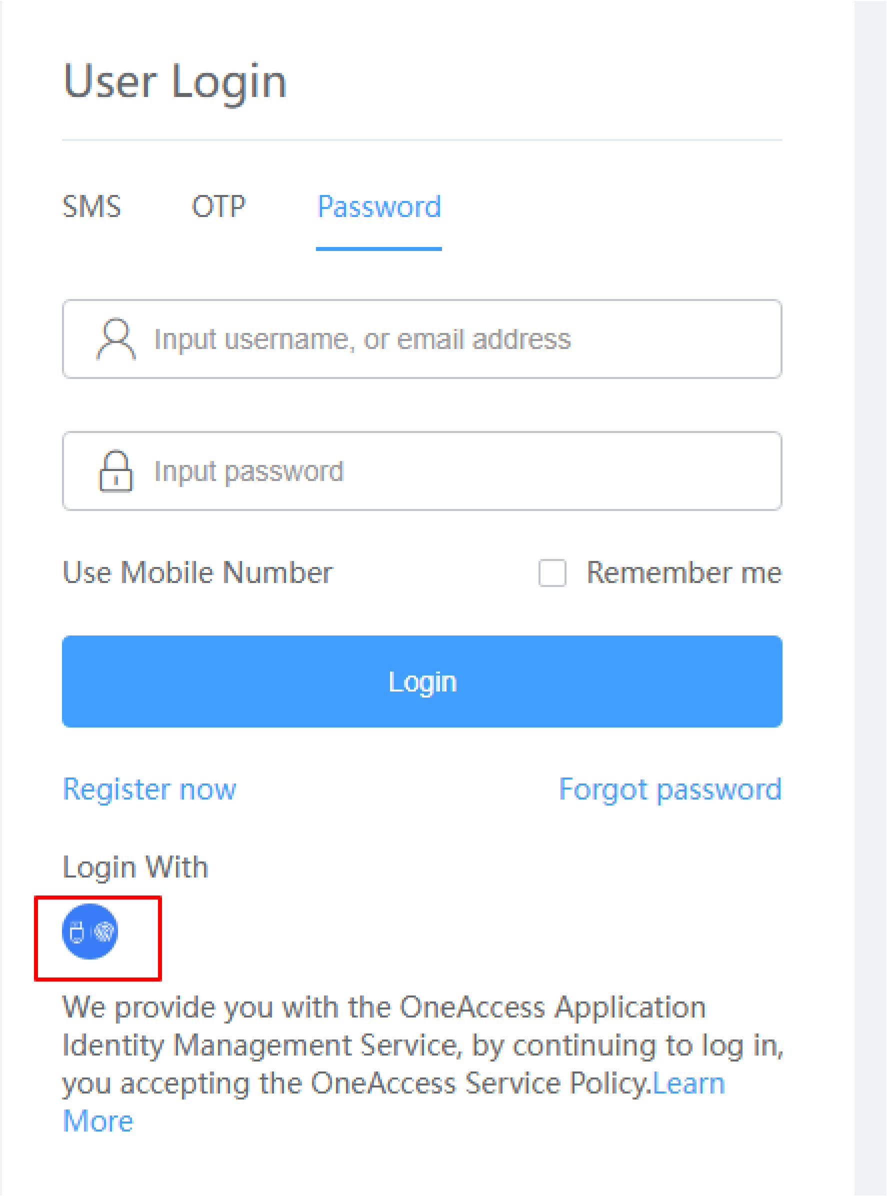
- If no security key or biometric authenticator is added, the bind button is grayed out
- You can bind multiple authenticators, or remove the added validator and add one again.

----End

Logging In to the User Portal Through FIDO2 Authentication

Go to the user portal page, and select the FIDO2 authentication mode for login. The security key or biometric authenticator is displayed. Complete the authentication.

Figure 5-3 Selecting the FIDO2 authentication mode



User Login

We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.Learn More

NOTE

In the traceless browser mode, biometric authenticators cannot be bound, which means FIDO2 authentication cannot be used in this mode.

5.2 Standard Protocol Authentication Providers

5.2.1 SAML Authentication

5.2.1.1 Configuring a SAML Authentication Provider

Introduction

OneAccess allows you to configure the SAML protocol as the authentication provider to log in to each application system for better user experience.

This section describes how to configure a SAML authentication provider.

Basic Concepts

- An identity provider (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.
- An service provider (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.
- Single sign-on (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 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.
- Security Assertion Markup Language 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.

Prerequisites

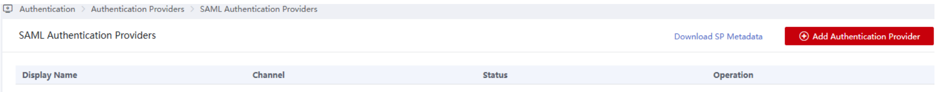
- You have permissions to access the administrator portal.
- You have the application system permission of the third-party identity provider (IDP) supporting SAML authentication.

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** > **Enterprise Authentication Providers**. Then click **SAML**.
3. On the **SAML Authentication Providers** page, click **Download SP Metadata** in the upper right corner. The metadata is automatically downloaded to the local PC.


Authentication > Authentication Providers > SAML Authentication Providers
SAML Authentication Providers
Download SP Metadata
Add Authentication Provider
Display Name
Channel
Status
Operation

Step 2 Upload the metadata file in **Step 1.3** to the enterprise IdP server. For details, see the documentation of the enterprise IdP.

Step 3 Obtain the metadata file of the enterprise IdP. For details, see the documentation of the enterprise IdP.

----End

Adding a SAML Authentication Provider

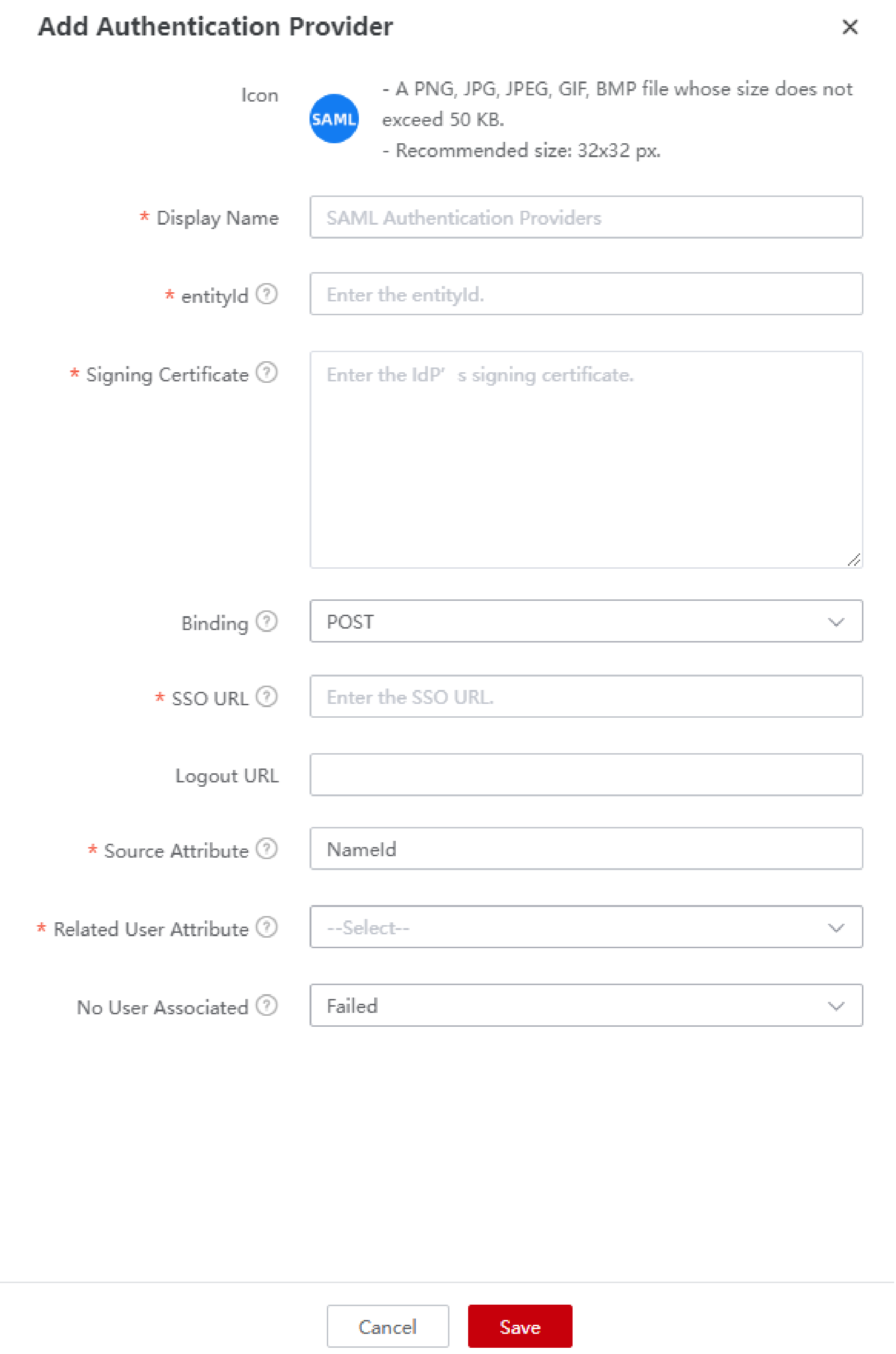
Add a SAML authentication provider and configure its metadata file in OneAccess to establish a trust on the IdP.

Step 1 Log in to the administrator portal.

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

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

Figure 5-4 Configuring parameters



Add Authentication Provider

Icon: SAML
- A PNG, JPG, JPEG, GIF, BMP file whose size does not exceed 50 KB.
- Recommended size: 32x32 px.

* Display Name: SAML Authentication Providers

* entityId: Enter the entityId.

* Signing Certificate: Enter the IdP' s signing certificate.

Binding: POST

* SSO URL: Enter the SSO URL.

Logout URL:

* Source Attribute: NameId

* Related User Attribute: --Select--

No User Associated: Failed

Table 5-2 Configuring 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.

Parameter	Mandatory	Description
Display Name	Yes	Display name of the authentication provider, for example, **SAML**.
entityId	Yes	Enter the value of **EntityID** displayed in the IdP's metadata file.
Signing Certificate	Yes	Obtain the signing certificate from the IdP's metadata file. A signing certificate is a public key certificate used for signature verification. It 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	Keep unique user attribute 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. For example, **Automatically create users**.

To map other attributes, such as username, set **No User Associated** to **Automatically create users**, and add the desired mappings to update existing attributes or not. For details, see **Table 5-3**.

Table 5-3 Mapping parameters

Parameter	Description
User Attribute	Attribute (such as username) in OneAccess that maps to the SAML.
Mapping Type	Mode of user attribute mapping between OneAccess and the SAML application. **NOTE** ● If **Mapping Type** is set to **Authentication Provider Attribute**, **Source Attribute** is required. ● If **Mapping Type** is set to **Fixed Attribute Value**, **Fixed Attribute Value** is required. ● If **Mapping Type** is set to **Script-based**, **Script** is required.

----End

5.2.1.2 Configuring SAML Authentication

Introduction

This section uses the OneAccess user portal as an example to describe how to configure the SAML authentication. After configuring the SAML authentication provider, you can refer to this section to log in to each application system.

Prerequisites

- You have permissions to access the administrator portal.
- You have configured the SAML authentication provider in OneAccess. For details, see **Configuring a SAML Authentication Provider**.

Enabling SAML Authentication

Step 1 Log in to the administrator portal.

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

Step 3 Click **User Portal** on the page.

Step 4 On the application information page, click the application icon.

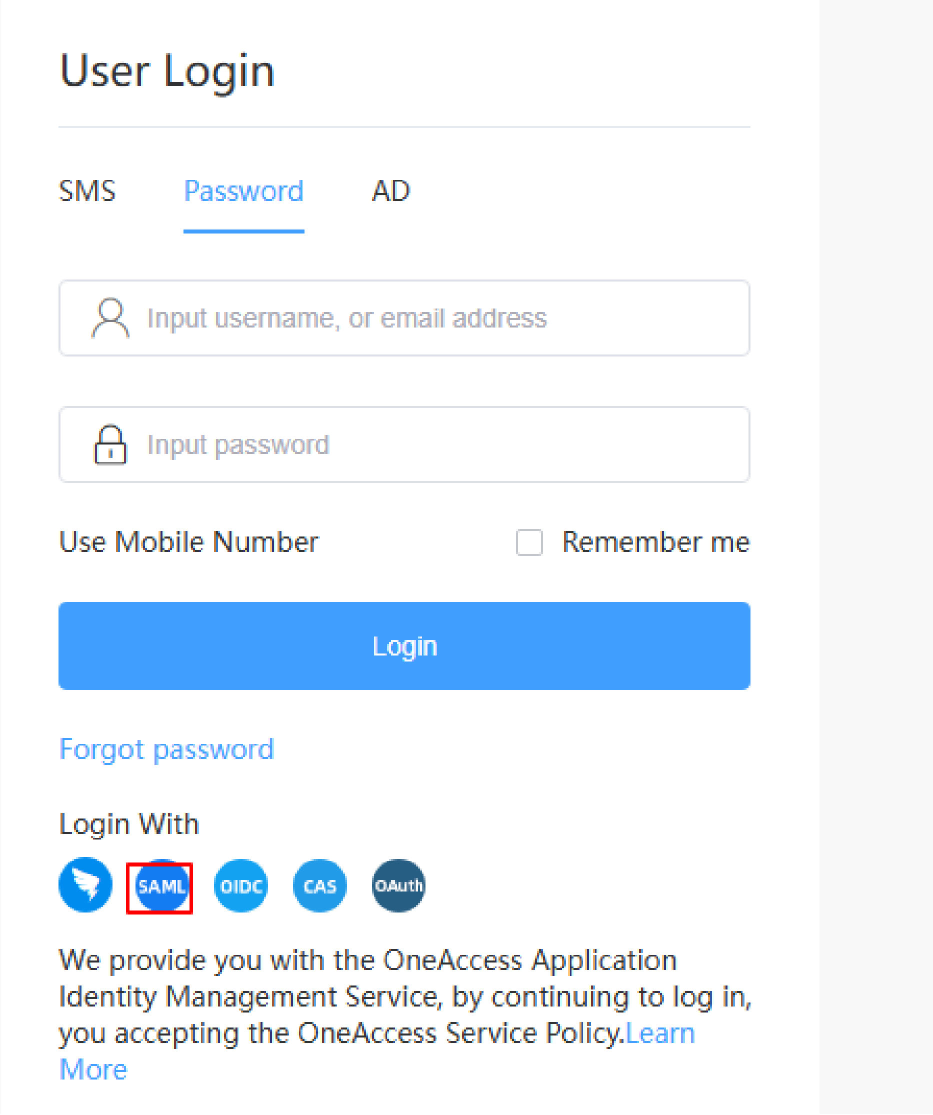
Step 5 Choose **Login Settings** > **Website Applications**, click ○ **SAML** to enable SAML authentication, and select the authentication provider added in **Adding a SAML Authentication Provider**.

----End

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 **Login**.

Figure 5-5 Selecting SAML



User Login

We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.Learn More

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 user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 5-2**.
- By default, users automatically created in the preceding scenario belong to the first root organization on the SP side.

----End

5.2.2 OIDC Authentication

5.2.2.1 Configuring an OIDC Authentication Provider

Introduction

OneAccess allows you to configure the OIDC protocol as the authentication provider to log in to each system for better login modes and experience.

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.

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.

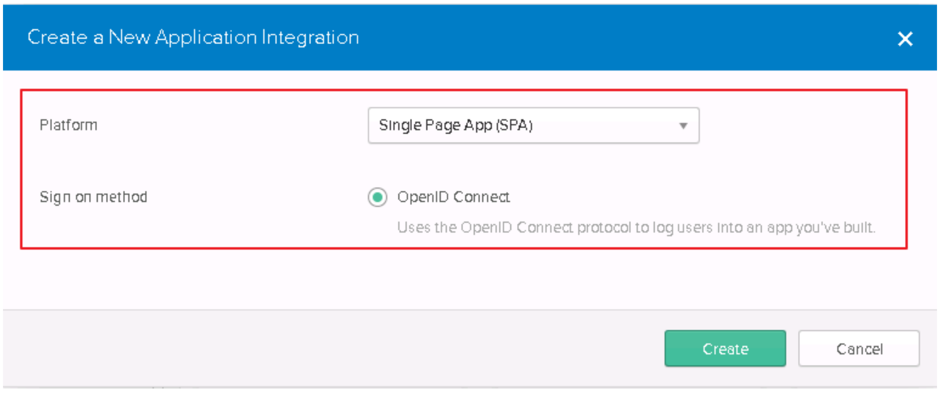
Step 1 Log in to the Okta platform.

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 5-4**. For example: https://xxx.huaweioneaccess.com/api/v1/oidc/sso/2***71-8***-D***1.

Figure 5-6 Configuring parameters

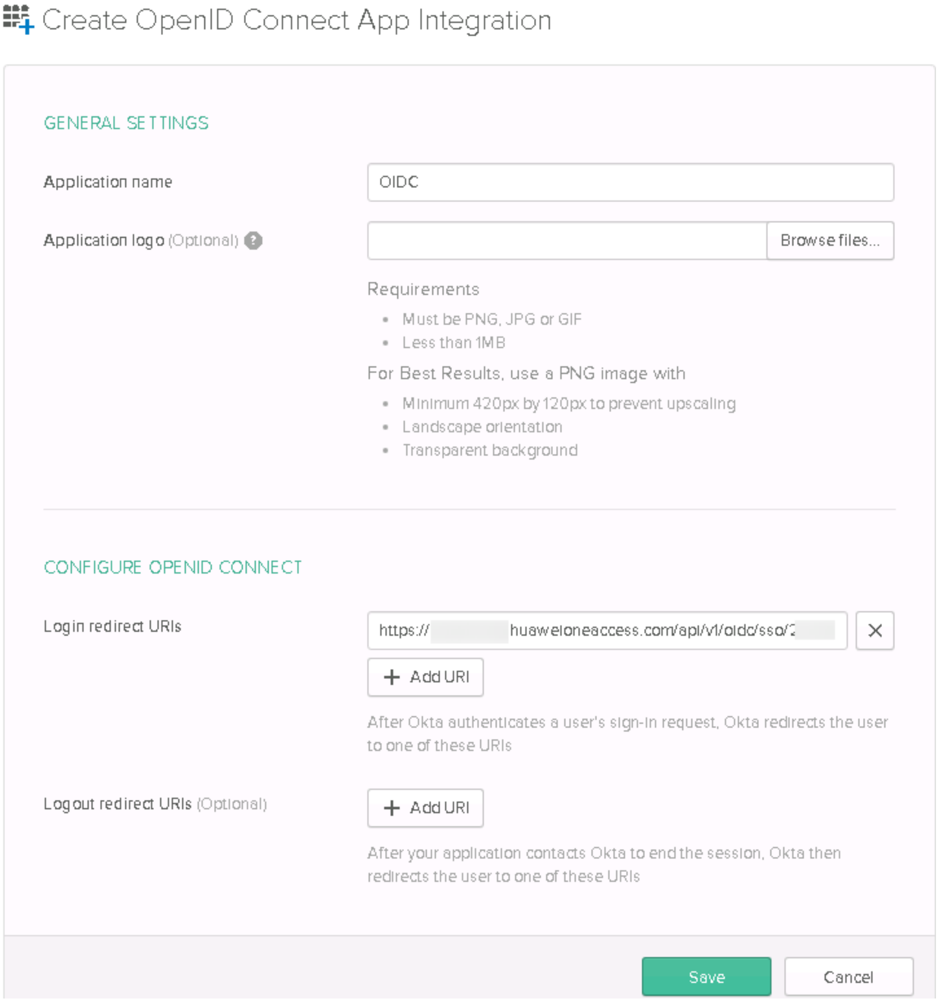


Create a New Application Integration

Platform: Single Page App (SPA)

Sign on method: ● OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

Figure 5-7 Configuring login redirect URIs



Create OpenID Connect App Integration

GENERAL SETTINGS

Application name: OIDC

Application logo (Optional)

Requirements

- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with

- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

CONFIGURE OPENID CONNECT

Login redirect URIs: https://[redacted]huaweioneaccess.com/api/v1/oidc/sso/[redacted]

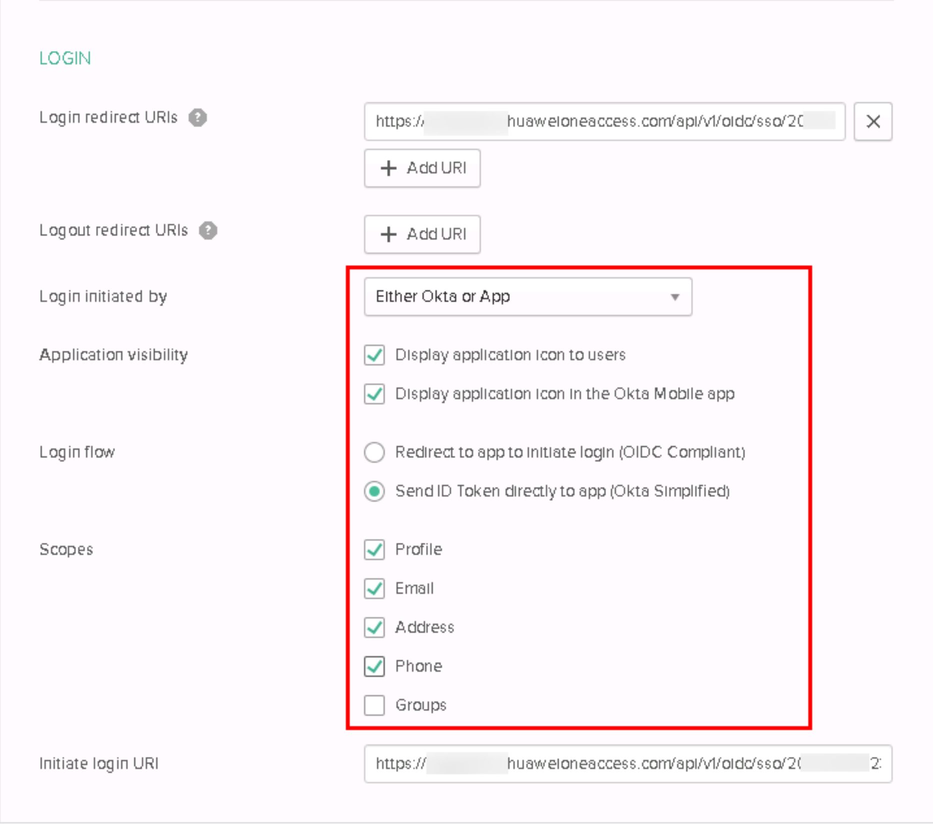
After Okta authenticates a user's sign-in request, Okta redirects the user to one of these URIs

Logout redirect URIs (Optional)

After your application contacts Okta to end the session, Okta then redirects the user to one of these URIs

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

Figure 5-8 Configuring application parameters



LOGIN

Login redirect URIs: https:/ huaweioneaccess.com/api/v1/oidc/sso/2(

+ Add URI

Logout redirect URIs: + Add URI

Login initiated by: Either Okta or App

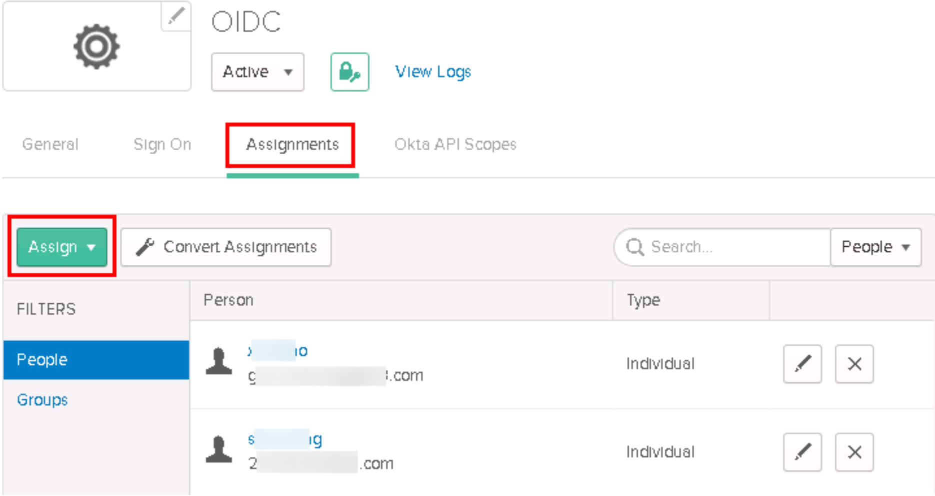
Application visibility:
☑ Display application icon to users
☑ Display application icon in the Okta Mobile app

Login flow:
○ Redirect to app to initiate login (OIDC Compliant)
● Send ID Token directly to app (Okta Simplified)

Scopes:
☑ Profile
☑ Email
☑ Address
☑ Phone
□ Groups

Initiate login URI: https:// huaweioneaccess.com/api/v1/oidc/sso/2(2:

Figure 5-9 Authorizing users



OIDC

Active ▾ View Logs

General | Sign On | Assignments | Okta API Scopes

Assign ▾ | Convert Assignments | Search... | People ▾

FILTERS
People
Groups

Person	Type
io .com	Individual
ig 2 .com	Individual

----End

Adding an OIDC Authentication Provider

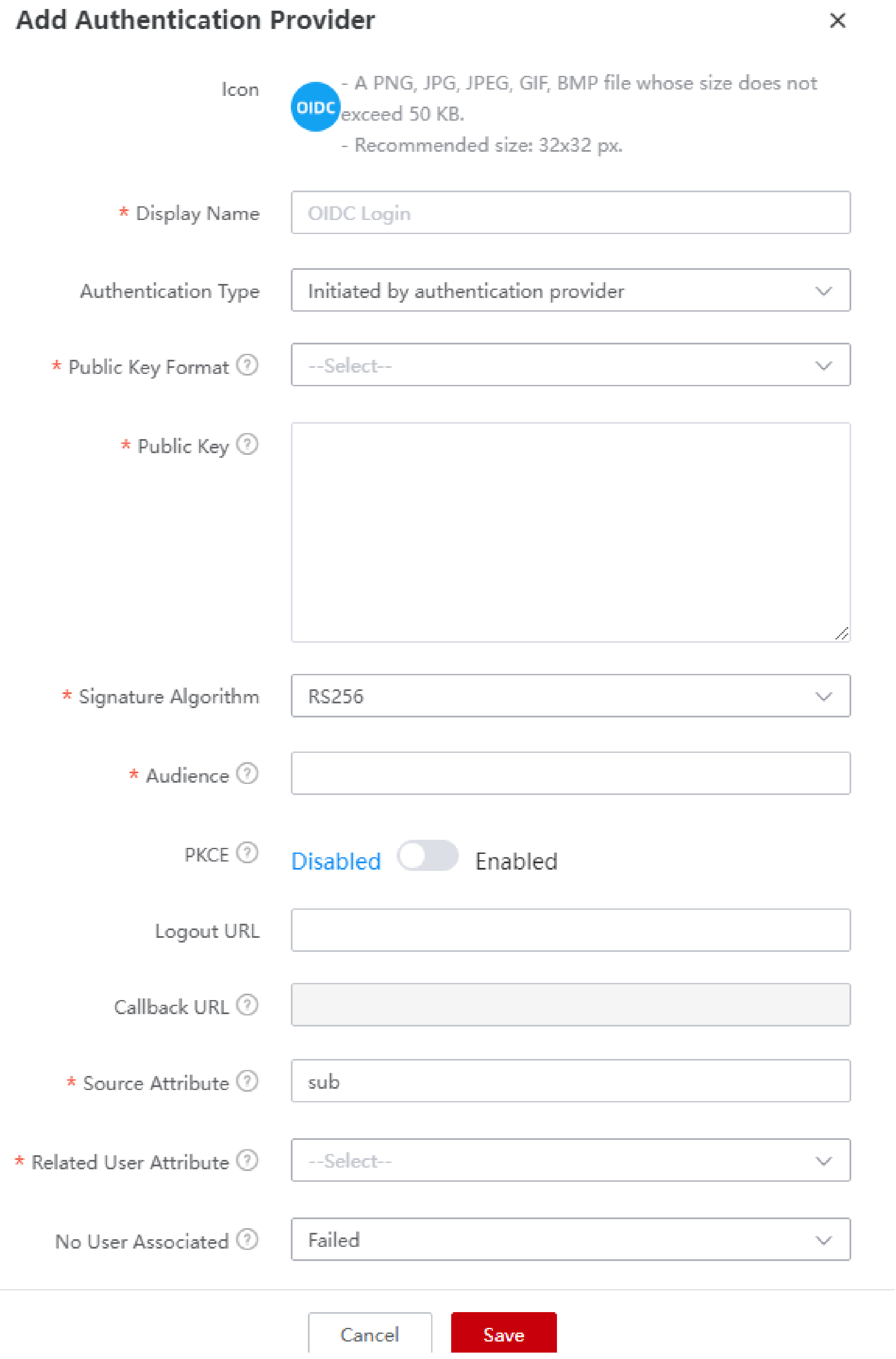
Add an OIDC authentication provider and configure the application information in OneAccess.

Step 1 Log in to the administrator portal.

Step 2 In the navigation pane, choose **Authentication** > **Authentication Providers** > **Enterprise Authentication Providers** > **OIDC**, and set parameters.

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

Figure 5-10 Configuring parameters



Add Authentication Provider

Icon: OIDC
- A PNG, JPG, JPEG, GIF, BMP file whose size does not exceed 50 KB.
- Recommended size: 32x32 px.

* Display Name	OIDC Login
Authentication Type	Initiated by authentication provider
* Public Key Format	--Select--
* Public Key	
* Signature Algorithm	RS256
* Audience	
PKCE	Disabled ○ Enabled
Logout URL	
Callback URL	
* Source Attribute	sub
* Related User Attribute	--Select--
No User Associated	Failed

Table 5-4 Configuring 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.
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.

Parameter	Mandatory	Description
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**.
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. For example, **Automatically create users**.

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 5-5**.

Table 5-5 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. **NOTE** ● If **Mapping Type** is set to **Authentication Provider Attribute**, **Source Attribute** is required. ● If **Mapping Type** is set to **Fixed Attribute Value**, **Fixed Attribute Value** is required. ● If **Mapping Type** is set to **Script-based**, **Script** is required.

----End

5.2.2.2 Configuring OIDC Authentication

Introduction

This section uses the OneAccess user portal as an example to describe how to configure the OIDC authentication. After configuring the OpenID Connect authentication source, you can refer to this section to log in to each application system.

Prerequisites

- You have permissions to access the administrator portal.
- You have configured the OIDC authentication provider in OneAccess. For details, see **Configuring an OIDC Authentication Provider**.

Enabling OIDC Authentication

Step 1 Log in to the administrator portal.

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

Step 3 Click **User Portal** on the page.

Step 4 On the application information page, click the application icon.

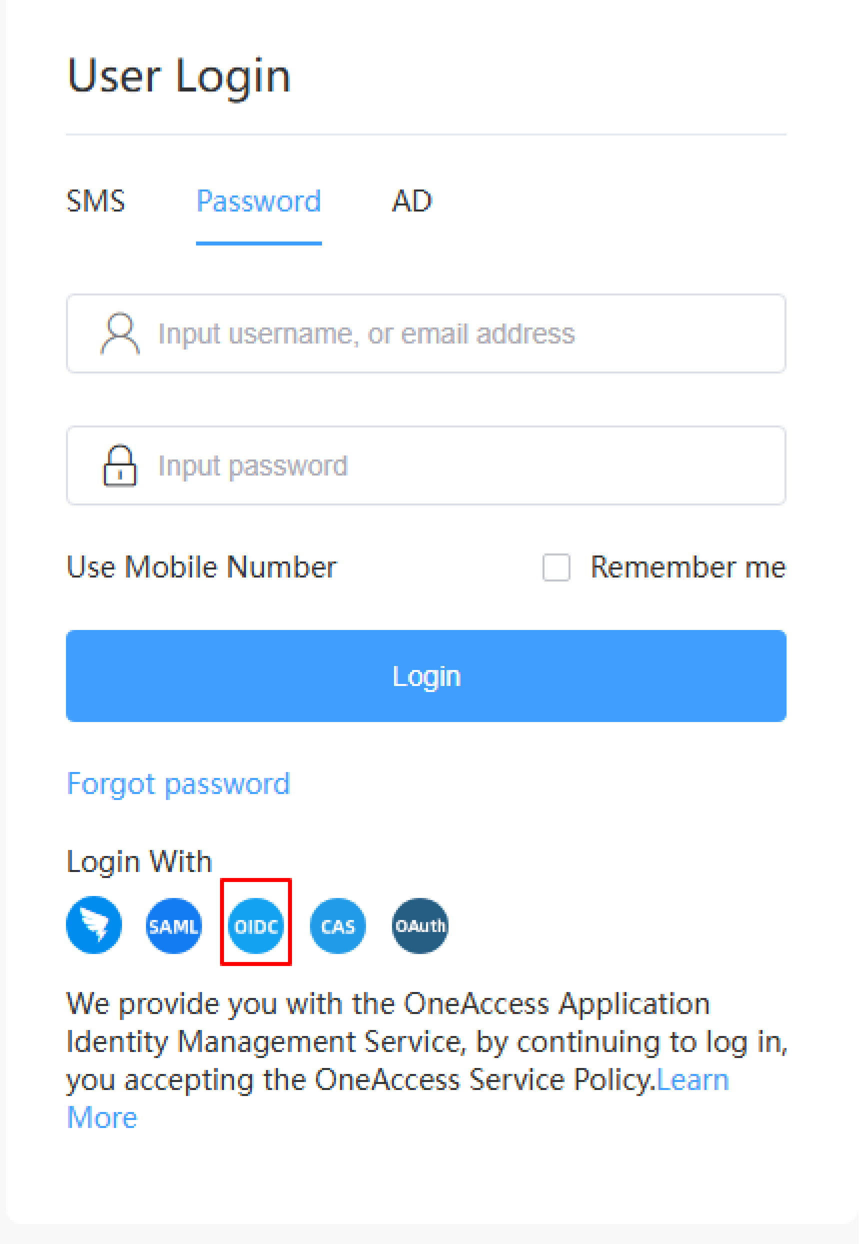
Step 5 Choose **Login Settings** > **Website Applications**, click **OIDC** to enable OIDC authentication, and select the authentication provider added in **Adding an OIDC Authentication Provider**.

----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 5-11 OIDC Authentication



User Login

SMS Password AD

Input username, or email address

Input password

Use Mobile Number □ Remember me

Login

Forgot password

Login With

We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.Learn More

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

NOTE

- To automatically create a user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 5-4**.
- If the user attribute **Email** is unique, users automatically created in the preceding scenario belong to the first root organization in OneAccess by default.

----End

5.2.3 CAS Authentication

5.2.3.1 Configuring a CAS Authentication Provider

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.

OneAccess allows you to configure the CAS protocol as the authentication provider. You can use the CAS protocol to log in to each application system and implement single sign-on (SSO) between application systems, providing simpler and more convenient login modes and better user experience for enterprise users.

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

Prerequisite

You have permissions to access the administrator portal.

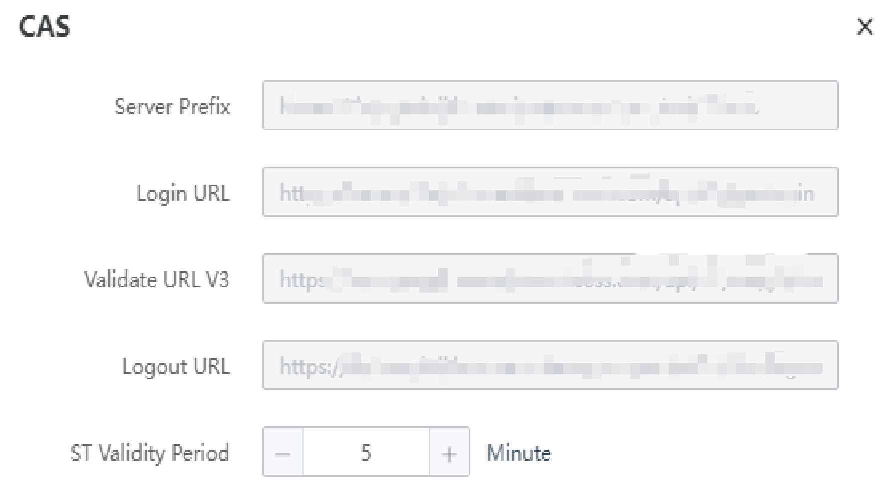
Establishing a Trust Between the Application and OneAccess

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. On the top navigation bar, choose **Settings** > **Service Settings**.
3. Click **CAS**.
4. On the **CAS** page, view the authentication address.

Figure 5-12 Viewing CAS configurations



CAS

Server Prefix [redacted]

Login URL [redacted]

Validate URL V3 [redacted]

Logout URL [redacted]

ST Validity Period 5 Minute

Table 5-6 Configuration parameters

Parameter	Description
Server Prefix	The value is automatically generated by the system and cannot be modified. Prefix of the CAS service address.
Login URL	The value is automatically generated by the system and cannot be modified. Login URL of the CAS service.
Validate URL V3	The value is automatically generated by the system and cannot be modified. URL used to validate tickets. The V3 address is recommended.
Logout URL	The value is automatically generated by the system and cannot be modified. URL for logging out of the CAS service.
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 5-7**.

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

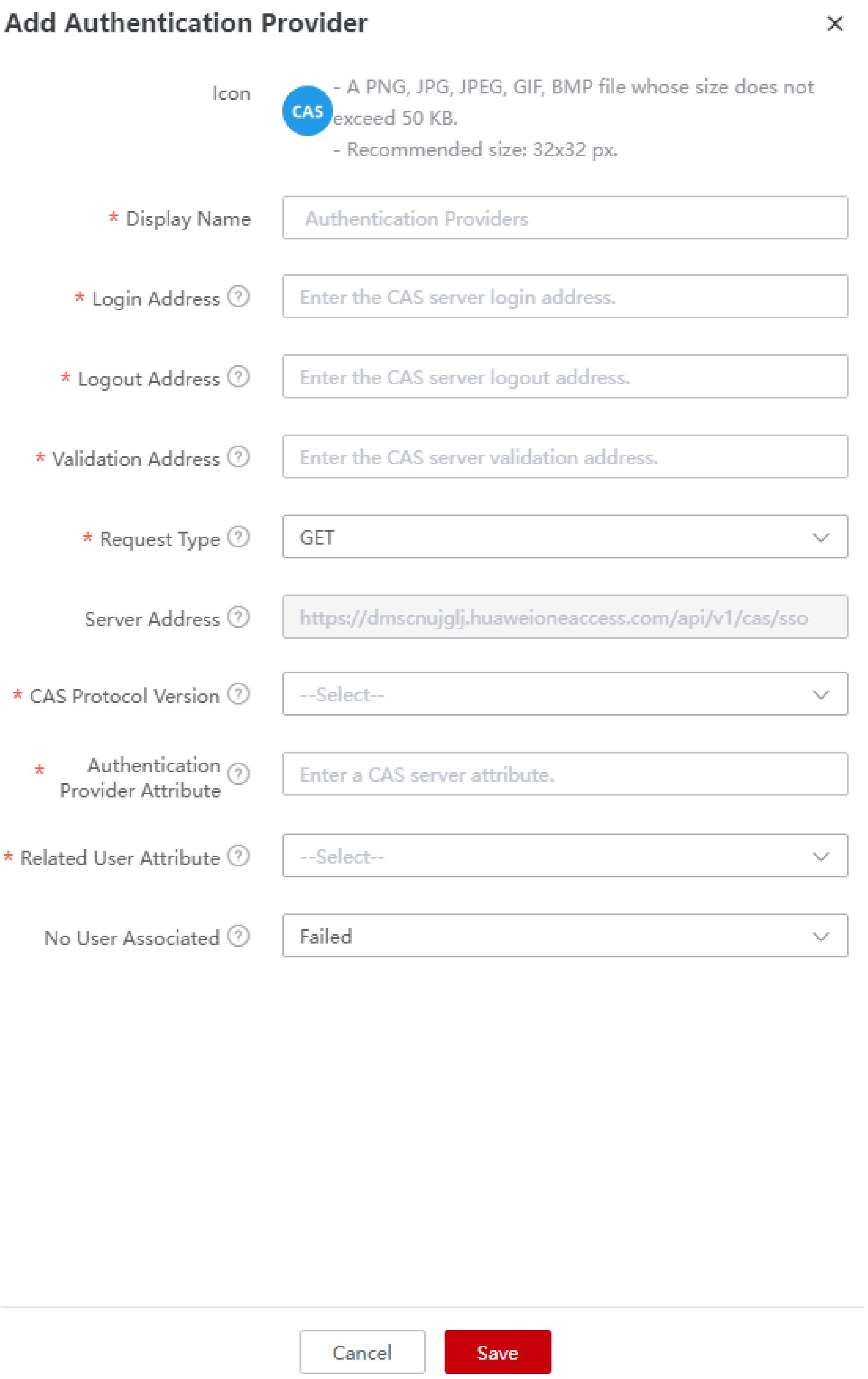
Add a CAS authentication provider and configure the application information in OneAccess.

Step 1 Log in to the administrator portal.

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

Step 3 Choose **Enterprise Authentication Providers** > **CAS**.

Step 4 On the **CAS Authentication Providers** page, click **Add Authentication Provider** in the upper right corner and set the parameters required.



Add Authentication Provider

Icon	CAS - A PNG, JPG, JPEG, GIF, BMP file whose size does not exceed 50 KB. - Recommended size: 32x32 px.
* Display Name	Authentication Providers
* Login Address	Enter the CAS server login address.
* Logout Address	Enter the CAS server logout address.
* Validation Address	Enter the CAS server validation address.
* Request Type	GET
Server Address	https://dmscnujglj.huaweioneaccess.com/api/v1/cas/sso
* CAS Protocol Version	--Select--
* Authentication Provider Attribute	Enter a CAS server attribute.
* Related User Attribute	--Select--
No User Associated	Failed

Table 5-7 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	Custom 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. The verification address of CAS 1.0 is *https://xxx.xxx.xxx/validate*. For details, see **Verifying Tickets (CAS 1.0)**. The verification address of CAS 2.0 is *https://xxx.xxx.xxx/serviceValidate*. For details, see **Verifying Tickets (CAS 2.0)**. The verification address of CAS 3.0 is *https://xxx.xxx.xxx/p3/serviceValidate*. For details, see **Verifying Tickets (CAS 3.0)**.
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. You can obtain this value when configuring the application.
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 click **Add Mapping**. For details, see **Table 5-8**.

Table 5-8 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. **NOTE** ● If **Mapping Type** is set to **Authentication Provider Attribute**, **Source Attribute** is required. ● If **Mapping Type** is set to **Fixed Attribute Value**, **Fixed Attribute Value** is required. ● If **Mapping Type** is set to **Script-based**, **Script** is required.

----End

5.2.3.2 Configuring CAS Authentication

Introduction

This section uses the OneAccess user portal as an example to describe how to configure the CAS authentication function. After configuring the CAS authentication provider in OneAccess, you can refer to this section to configure CAS authentication for logging in to each application system.

Prerequisites

- You have permissions to access the administrator portal.
- You have configured the CAS authentication provider in OneAccess by referring to **Configuring a CAS Authentication Provider**.

Enabling CAS Authentication

Step 1 Log in to the administrator portal.

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

Step 3 Click **User Portal** on the page.

Step 4 On the application information page, click the application icon.

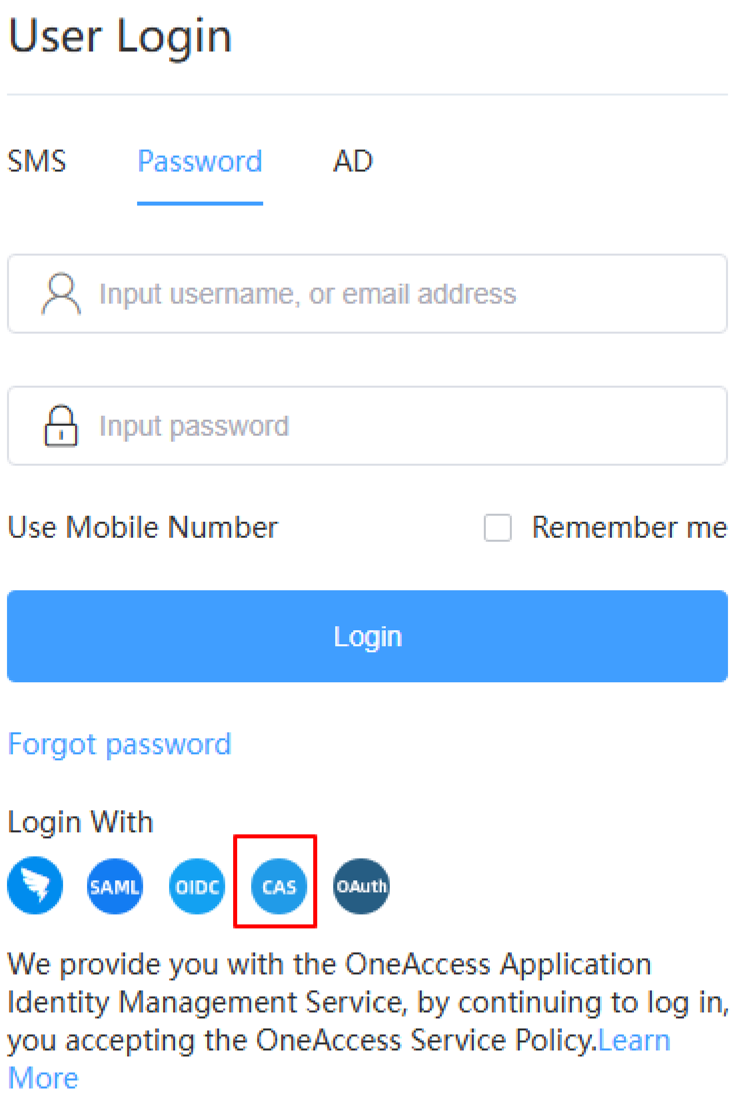
Step 5 Choose **Login Settings** > **Web Applications**, click ○ in the **Operation** column of **CAS** to enable CAS authentication, and select the authentication provider added in **Adding a CAS Authentication Provider**.

----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 **Login**.

Figure 5-13 Selecting CAS



User Login

We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.Learn More

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 user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 5-7**.
- By default, users automatically created in the preceding scenario belong to the first root organization in OneAccess.

----End

5.2.4 OAuth Authentication

5.2.4.1 Configuring an OAuth Authentication Provider

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.

OneAccess allows you to configure the OAuth protocol as the authentication provider. You can use the OAuth protocol to log in to each application system, providing simpler and more convenient login modes and better user experience for enterprise users.

This section describes how to configure an OAuth authentication provider.

Prerequisite

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. On the top navigation bar, choose **Settings** > **Service Settings**.
3. Click **OIDC**.
4. On the **OIDC** page, view the authentication address. Click **OIDC Settings** in the upper right corner to view the configured authentication parameters.

Step 2 Obtain the callback address in OneAccess. For details, see **Table 5-9**.

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 an OAuth Authentication Provider

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

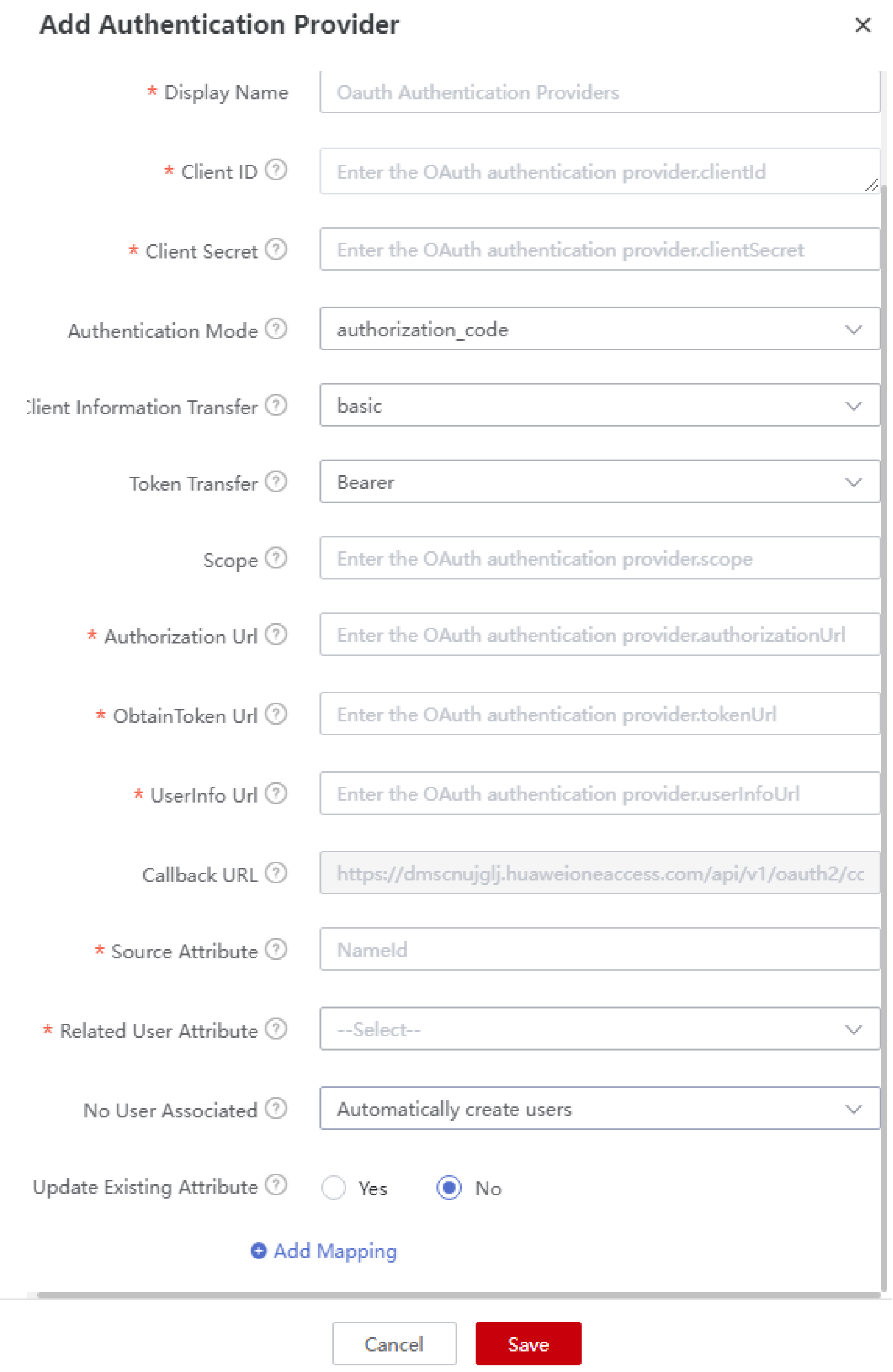
Step 1 Log in to the administrator portal.

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

Step 3 Choose **Enterprise Authentication Providers** > **OAuth**.

Step 4 On the **OAuth Authentication Providers** page, click **Add Authentication Provider** in the upper right corner and set the parameters required.

Figure 5-14 Configuration parameters



Add Authentication Provider ×

* Display Name	Oauth Authentication Providers
* Client ID ⓘ	Enter the OAuth authentication provider.clientId
* Client Secret ⓘ	Enter the OAuth authentication provider.clientSecret
Authentication Mode ⓘ	authorization_code
:lient Information Transfer ⓘ	basic
Token Transfer ⓘ	Bearer
Scope ⓘ	Enter the OAuth authentication provider.scope
* Authorization Url ⓘ	Enter the OAuth authentication provider.authorizationUrl
* ObtainToken Url ⓘ	Enter the OAuth authentication provider.tokenUrl
* UserInfo Url ⓘ	Enter the OAuth authentication provider.userInfoUrl
Callback URL ⓘ	https://dmscnujglj.huaweioneaccess.com/api/v1/oauth2/cc
* Source Attribute ⓘ	NameId
* Related User Attribute ⓘ	--Select--
No User Associated ⓘ	Automatically create users
Update Existing Attribute ⓘ	○ Yes ● No

Table 5-9 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**.
Client ID	Yes	Client ID of the application. Obtain the value from the application.
Client Secret	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.

Parameter	Mandatory	Description
Update Existing Attribute	Yes	Default value: **No**. 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 click **Add Mapping**. For details, see **Table 5-10**.

Table 5-10 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. **NOTE** ● If **Mapping Type** is set to **Authentication Provider Attribute**, **Source Attribute** is required. ● If **Mapping Type** is set to **Fixed Attribute Value**, **Fixed Attribute Value** is required. ● If **Mapping Type** is set to **Script-based**, **Script** is required.

----End

5.2.4.2 Configuring OAuth Authentication

Introduction

This section uses the OneAccess user portal as an example to describe how to configure the OAuth authentication function. After configuring the OAuth authentication provider in OneAccess, you can refer to this section to configure OAuth authentication for logging in to each application system.

Prerequisites

- You have permissions to access the administrator portal.
- You have configured the OAuth authentication provider in OneAccess by referring to **Configuring an OAuth Authentication Provider**.

Enabling OAuth Authentication

Step 1 Log in to the administrator portal.

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

Step 3 Click **User Portal** on the page.

Step 4 On the application information page, click the application icon.

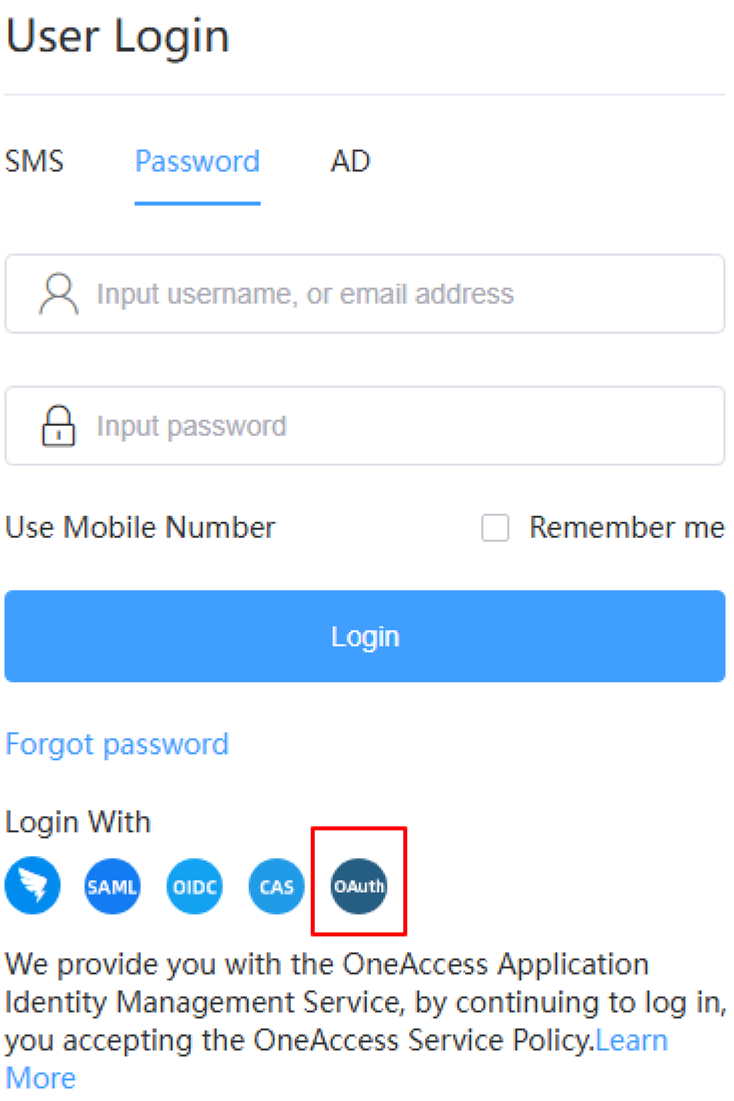
Step 5 Choose **Login Settings** > **Web Applications**, click ○ in the **Operation** column of **OAuth** to enable OAuth authentication, and select the authentication provider added in **Adding an OAuth Authentication Provider**.

----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 **Login**.

Figure 5-15 Selecting OAuth



User Login

We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.Learn More

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 user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 5-9**.
- By default, users automatically created in the preceding scenario belong to the first root organization in OneAccess.

----End

5.2.5 Kerberos Authentication

5.2.5.1 Configuring a Kerberos Authentication Provider

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**.

Active Directory (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.

OneAccess allows you to configure the Kerberos protocol as the authentication provider. You can use the Kerberos protocol to log in to each application system, providing simpler and more convenient login modes and better user experience for enterprise users.

This section describes how to configure a Kerberos authentication provider.

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**.

NOTE

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

NOTE

Check whether AES 256-bit encryption is enabled for each AD user who requires password-free login. The procedure is as follows:

On the AD server, right-click the user to open the property dialog box. Find the account properties and ensure that **This account supports Kerberos AES 256-bit encryption** is selected.

----End

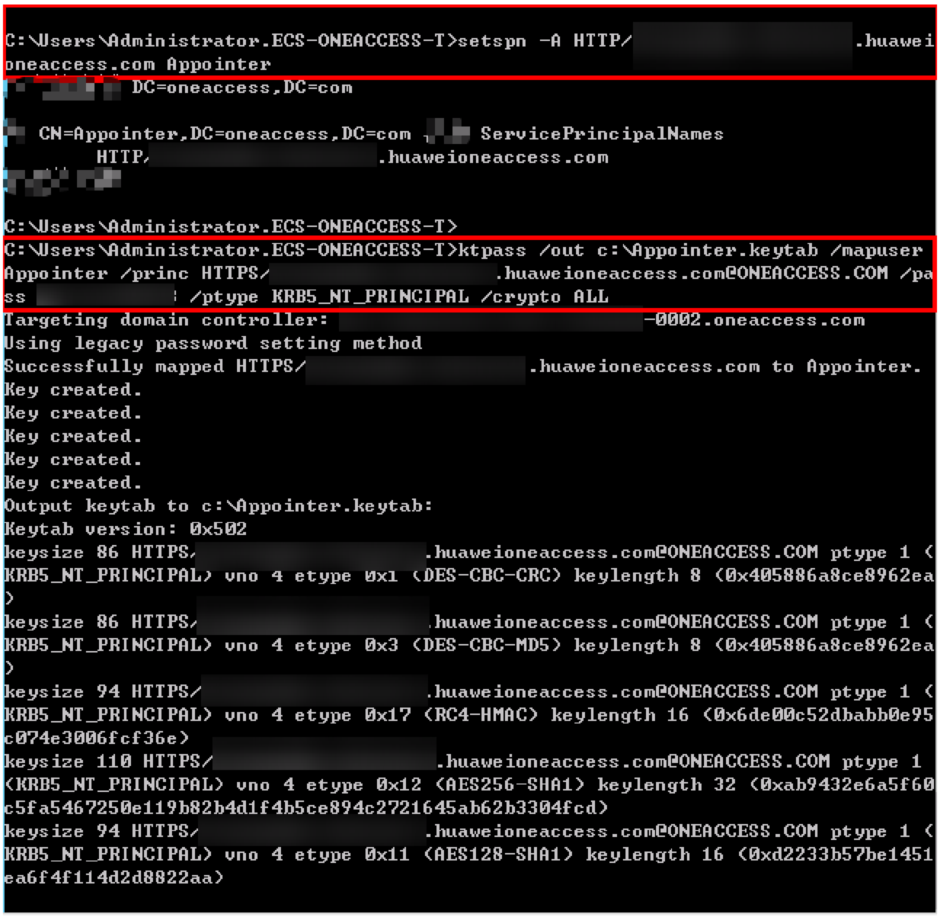
Configuring the AD Server

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 AES256-SHA1**" 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 AES256-SHA1**.



```
C:\Users\Administrator.ECS-ONEACCESS-T>setspn -A HTTP/[redacted].huawei
oneaccess.com Appointer
[redacted] DC=oneaccess,DC=com

[redacted] CN=Appointer,DC=oneaccess,DC=com [redacted] ServicePrincipalNames
        HTTP/[redacted].huaweioneaccess.com
[redacted]

C:\Users\Administrator.ECS-ONEACCESS-T>
C:\Users\Administrator.ECS-ONEACCESS-T>ktpass /out c:\Appointer.keytab /mapuser
Appointer /princ HTTPS/[redacted].huaweioneaccess.com@ONEACCESS.COM /pa
ss [redacted] /ptype KRB5_NT_PRINCIPAL /crypto ALL
Targeting domain controller: [redacted]-0002.oneaccess.com
Using legacy password setting method
Successfully mapped HTTPS/[redacted].huaweioneaccess.com to Appointer.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to c:\Appointer.keytab:
Keytab version: 0x502
keysize 86 HTTPS/[redacted].huaweioneaccess.com@ONEACCESS.COM ptype 1 (
KRB5_NT_PRINCIPAL) vno 4 etype 0x1 (DES-CBC-CRC) keylength 8 (0x405886a8ce8962ea
)
keysize 86 HTTPS/[redacted].huaweioneaccess.com@ONEACCESS.COM ptype 1 (
KRB5_NT_PRINCIPAL) vno 4 etype 0x3 (DES-CBC-MD5) keylength 8 (0x405886a8ce8962ea
)
keysize 94 HTTPS/[redacted].huaweioneaccess.com@ONEACCESS.COM ptype 1 (
KRB5_NT_PRINCIPAL) vno 4 etype 0x17 (RC4-HMAC) keylength 16 (0x6de00c52dbabb0e95
c074e3006fcf36e)
keysize 110 HTTPS/[redacted].huaweioneaccess.com@ONEACCESS.COM ptype 1
(KRB5_NT_PRINCIPAL) vno 4 etype 0x12 (AES256-SHA1) keylength 32 (0xab9432e6a5f60
c5fa5467250e119b82b4d1f4b5ce894c2721645ab62b3304fcd)
keysize 94 HTTPS/[redacted].huaweioneaccess.com@ONEACCESS.COM ptype 1 (
KRB5_NT_PRINCIPAL) vno 4 etype 0x11 (AES128-SHA1) keylength 16 (0xd2233b57be1451
ea6f4f114d2d8822aa)
```

Step 3 Configure an appointment in the AD server.

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

----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}*.

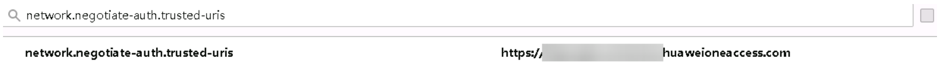
- Google Chrome

  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}*.



network.negotiate-auth.trusted-uris

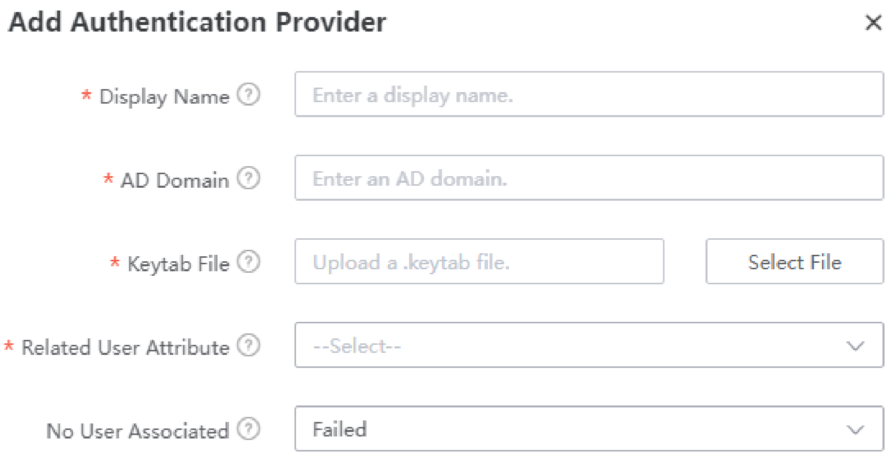
network.negotiate-auth.trusted-uris https://[redacted]huaweioneaccess.com

Adding a Kerberos Authentication Provider

Step 1 Log in to the administrator portal.

Step 2 On the top navigation bar, 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 5-16 Adding an authentication provider



Add Authentication Provider

* Display Name: Enter a display name.

* AD Domain: Enter an AD domain.

* Keytab File: Upload a .keytab file.

* Related User Attribute: --Select--

No User Associated: Failed

Table 5-11 Configuration parameters

Parameter	Description
* Display Name	Custom 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 On the top navigation bar, 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.

----End

5.2.5.2 Configuring Kerberos Authentication

Introduction

This section uses the OneAccess user portal as an example to describe how to configure the Kerberos authentication function. After configuring the Kerberos authentication provider in OneAccess, you can refer to this section to configure Kerberos authentication for logging in to each application system.

Prerequisites

- You have permissions to access the administrator portal.
- You have configured the Kerberos authentication provider in OneAccess by referring to **Configuring a Kerberos Authentication Provider**.

Enabling Kerberos Authentication

Step 1 Log in to the administrator portal.

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

Step 3 Click **User Portal** on the page.

Step 4 On the application information page, click the application icon.

Step 5 Choose **Login Settings** > **Web Applications**, click in the **Operation** column of **Kerberos** to 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

Logging In to the User Portal Through Kerberos Authentication

Step 1 Log in to the AD domain.

Step 2 Access the user portal using a browser without entering a password. The user is the user for logging in to the AD domain in **Creating an AD User**.

----End

5.2.6 AD Authentication

5.2.6.1 Configuring an AD Authentication Provider

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

To facilitate user authentication, OneAccess uses LDAP to direct the authentication to the AD domain. After the AD authentication succeeds, OneAccess matches the user attributes returned by the AD domain with the user association attributes in OneAccess. If the authentication is successful, the user can log in to OneAccess.

This section describes how to configure an AD authentication provider.

Prerequisite

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.

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.)

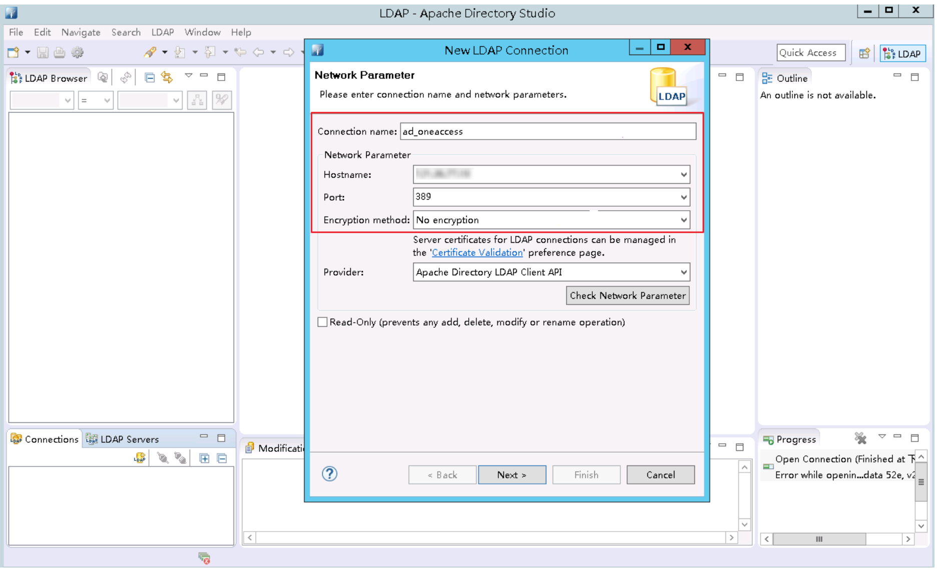
----End

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.

Figure 5-17 Creating a connection



LDAP - Apache Directory Studio
File Edit Navigate Search LDAP Window Help
LDAP Browser
Connections
LDAP Servers
Modificati
Quick Access
LDAP
Outline
An outline is not available.
Progress
Open Connection (Finished at
Error while openin...data 52e, v2
New LDAP Connection
< Back
Next >
Finish
Cancel

Network Parameter

Please enter connection name and network parameters.

Connection name: ad_oneaccess

Network Parameter

Hostname: [redacted]

Port: 389

Encryption method: No encryption

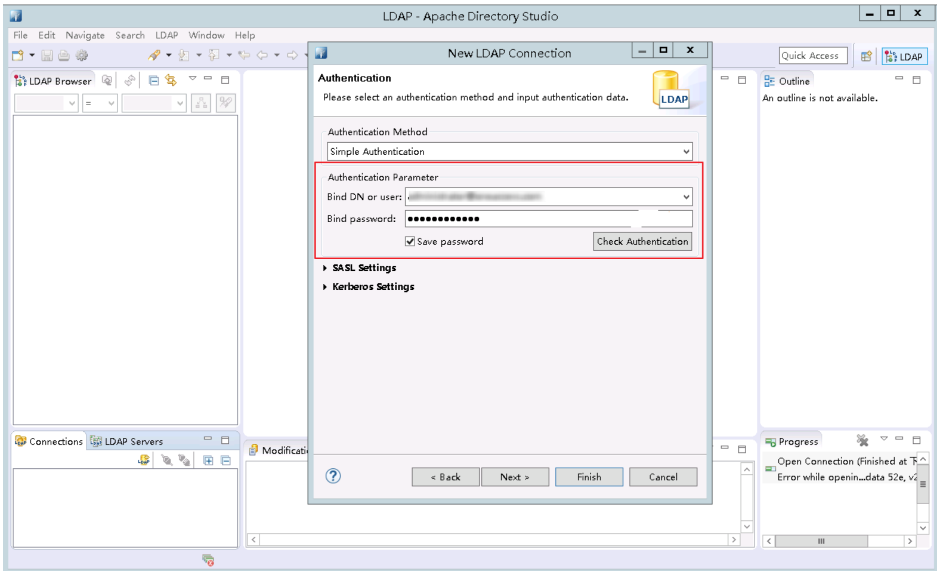
Server certificates for LDAP connections can be managed in the 'Certificate Validation' preference page.

Provider: Apache Directory LDAP Client API

Check Network Parameter

□ Read-Only (prevents any add, delete, modify or rename operation)

Figure 5-18 Setting parameters



LDAP - Apache Directory Studio

New LDAP Connection

Authentication

Please select an authentication method and input authentication data.

Authentication Method: Simple Authentication

Authentication Parameter

Bind DN or user:

Bind password: ●●●●●●●●●●●●

☑ Save password

----End

Adding an AD Authentication Provider

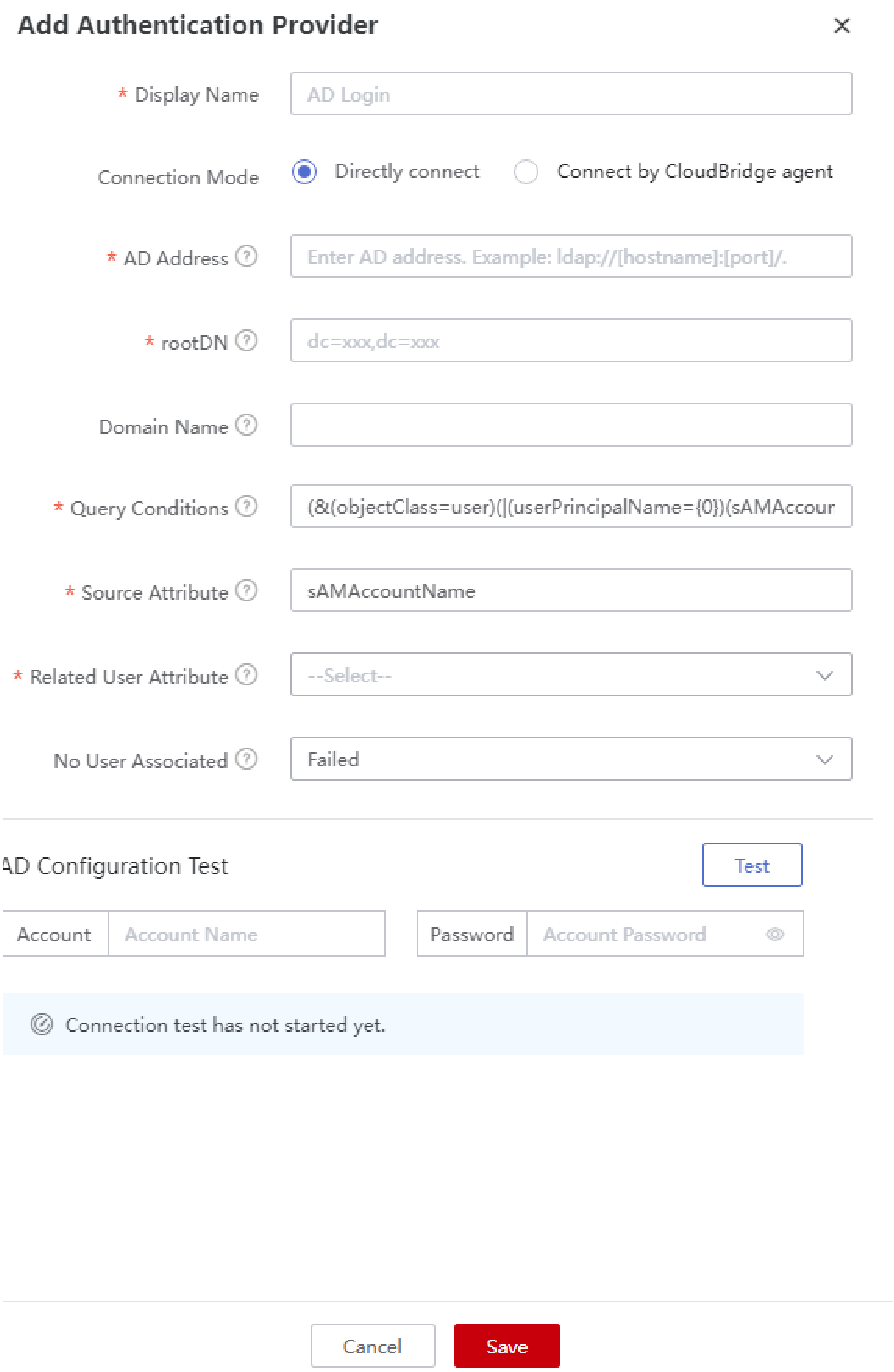
Step 1 Log in to the administrator portal.

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

Step 3 Choose **Enterprise Authentication Providers** > **AD**.

Step 4 On the **AD Authentication Providers** page, click **Add Authentication Provider** in the upper right corner and set the parameters required.

Figure 5-19 Setting parameters



Add Authentication Provider

* Display Name: AD Login

Connection Mode: ● Directly connect ○ Connect by CloudBridge agent

* AD Address: Enter AD address. Example: ldap://[hostname]:[port]/.

* rootDN: dc=xxx,dc=xxx

Domain Name:

* Query Conditions: (&(objectClass=user)(|(userPrincipalName={0})(sAMAccour

* Source Attribute: sAMAccountName

* Related User Attribute: --Select--

No User Associated: Failed

AD Configuration Test

Account: Account Name

Password: Account Password

Connection test has not started yet.

Table 5-12 Configuration parameters

Parameter	Description
Display Name	Mandatory. Display name of the authentication provider, for example, **AD**.

Parameter	Description
Connection Mode	You can choose **Directly connect** (default) or **Connect by CloudBridge agent**.
AD Address	Mandatory. 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	Mandatory. 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	Mandatory. 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	Mandatory. 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	Mandatory. User attribute mapped by AD in the system. The user attribute must be a unique text.
No User Associated	Mandatory. Operation that will be performed if a user logs in successfully but fails to be associated with a system user.

NOTE

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

----End

Enabling AD Authentication

Step 1 On the top navigation bar, choose **Resources** > **Applications**.

Step 2 On the **Applications** page, click **User Portal**.

Step 3 Click the user portal icon to go to the general information page.

Step 4 Choose **Login Settings** > **Web Applications**, click in the **Operation** column of **AD** to enable AD authentication, and select the authentication provider added in **Adding an AD Authentication Provider**.

NOTE

When AD authentication is enabled, the password login mode text box is used. You need to click in the **Operation** column of **Password** to disable the database authentication mode. If LDAP authentication is enabled, click in the **Operation** column of **LDAP** to disable LDAP authentication.

----End

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?
   a. Check whether the Netlogon and DFS services have been started.
   b. 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.
   c. For the AD domain, check the logs in the event viewer and use the Dcdiag tool to locate the error.
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}*".

5.2.6.2 Configuring AD Authentication

Introduction

This section uses the OneAccess user portal as an example to describe how to configure the AD authentication function. After configuring the AD authentication provider in OneAccess, you can refer to this section to configure AD authentication for logging in to each application system.

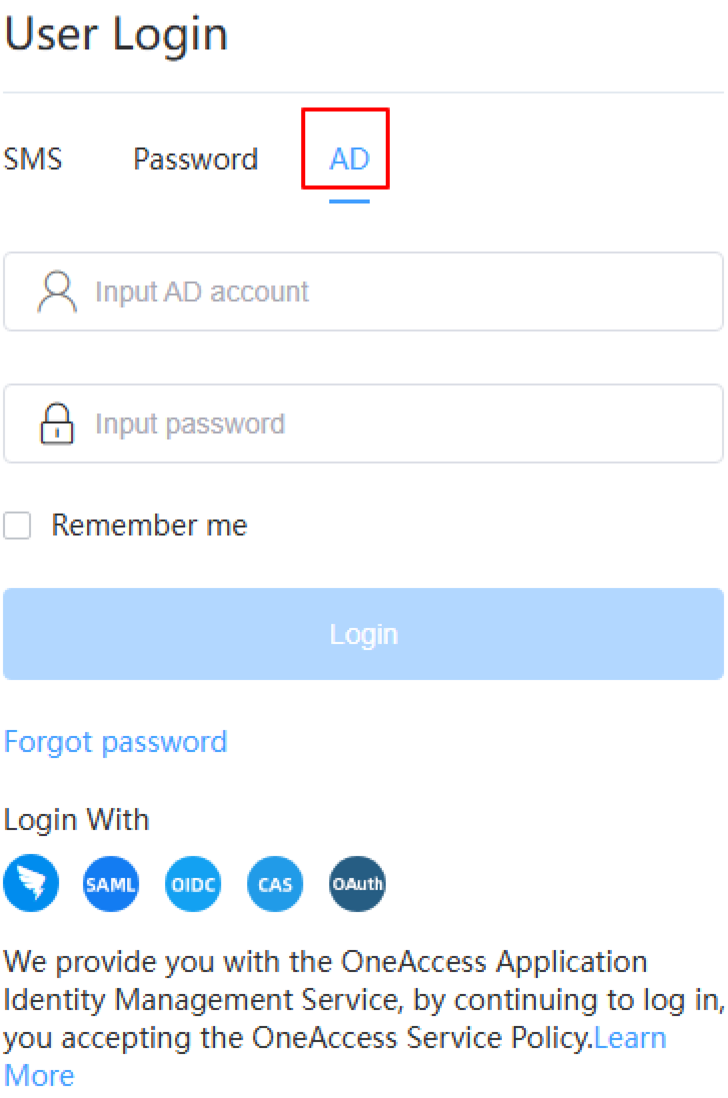
Prerequisites

- You have permissions to access the administrator portal.
- You have configured the AD authentication provider in OneAccess by referring to **Configuring an AD Authentication Provider**.

Logging In to the User Portal Through AD Authentication

1. On the user portal login page, select **AD**, enter an AD account and password, and click **Login**.

Figure 5-20 Selecting AD



User Login

□ Remember me

We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.Learn More

2. After login, go to the administrator portal, choose **Users** > **Organizations and Users**, and view the automatically created user.
3. If the AD user is not associated with any OneAccess user and you have set **No User Associated** to **Failed** (see **Figure 5-19**), the login will fail. To ensure successful login, create a user with the same name as the AD user in OneAccess.

5.2.7 LDAP Authentication

5.2.7.1 Configuring an LDAP Authentication Provider

Introduction

Lightweight Directory Access Protocol (LDAP) is a 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 internal networks of their company after logging in on a PC for once.

Table 5-13 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.

To facilitate enterprise user authentication, OneAccess uses LDAP to direct authentication to LDAP. After LDAP authentication succeeds, OneAccess matches the user attributes returned by LDAP with the associated attributes of IDaaS users. If the authentication is successful, the user can log in to OneAccess.

This section describes how to configure an LDAP authentication provider.

Prerequisite

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.

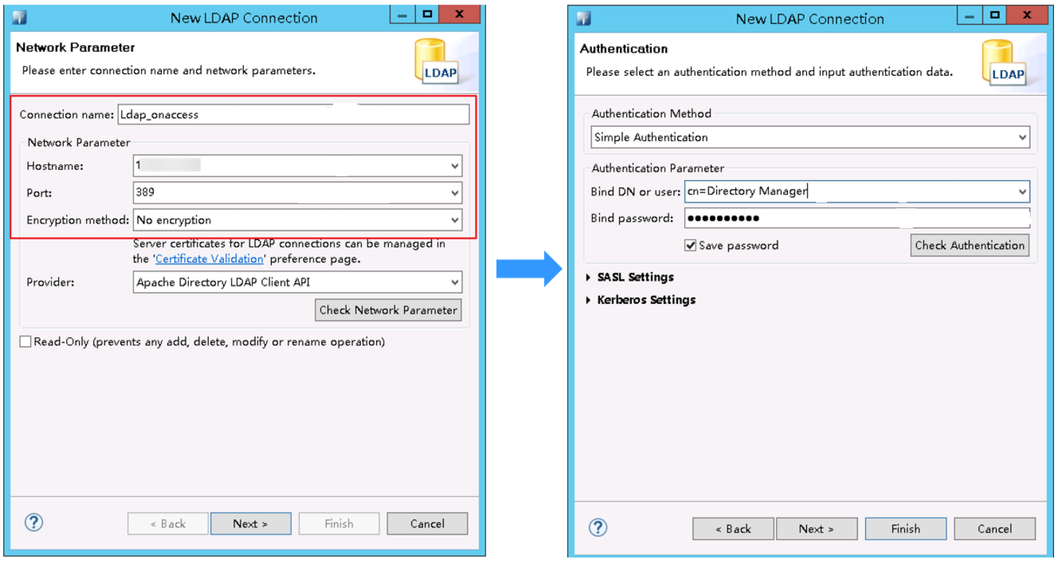
----End

Configuring LDAP Connection

Step 1 Download and install ApacheDirectoryStudio, an LDAP client.

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

Figure 5-21 Creating a connection



New LDAP Connection

Network Parameter

Please enter connection name and network parameters.

Connection name: Ldap_onaccess

Network Parameter

Hostname: 1[redacted]

Port: 389

Encryption method: No encryption

Server certificates for LDAP connections can be managed in the 'Certificate Validation' preference page.

Provider: Apache Directory LDAP Client API

☐ Read-Only (prevents any add, delete, modify or rename operation)

New LDAP Connection

Authentication

Please select an authentication method and input authentication data.

Authentication Method: Simple Authentication

Authentication Parameter

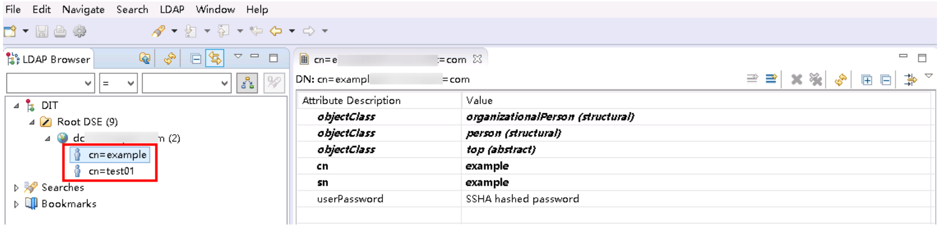
Bind DN or user: cn=Directory Manager

Bind password: ●●●●●●●●●●●

☑ Save password

Step 3 Add an account in LDAP.

Figure 5-22 Viewing users



- DIT
  - Root DSE (9)
    - dc[redacted]n (2)
      - cn=example
      - cn=test01
- Searches
- Bookmarks

cn=e[redacted]=com

DN: cn=exampl[redacted]=com

Attribute Description	Value
objectClass	***organizationalPerson (structural)***
objectClass	***person (structural)***
objectClass	***top (abstract)***
cn	**example**
sn	**example**
userPassword	SSHA hashed password

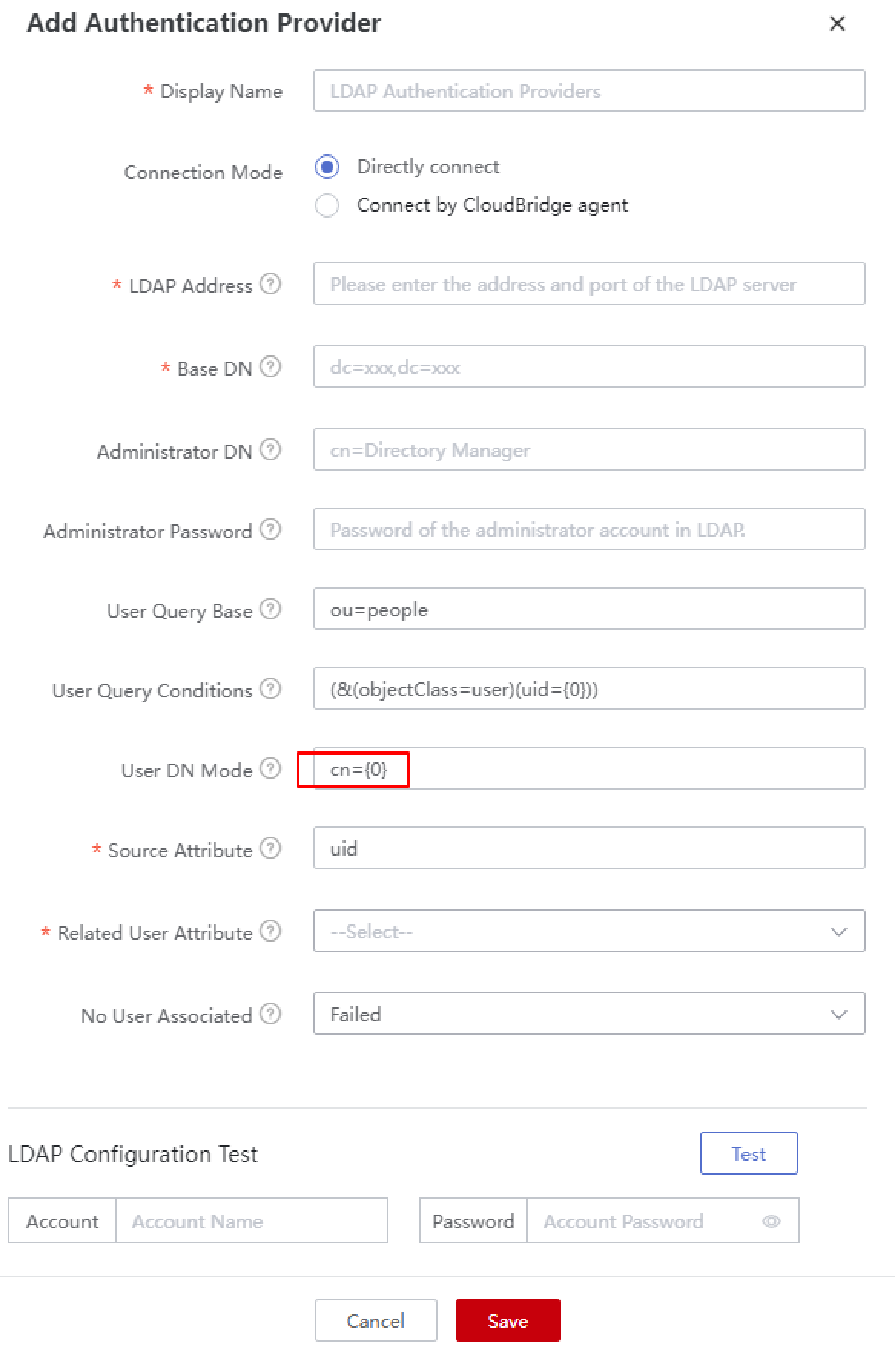
----End

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.

Figure 5-23 DN authentication mode



Add Authentication Provider

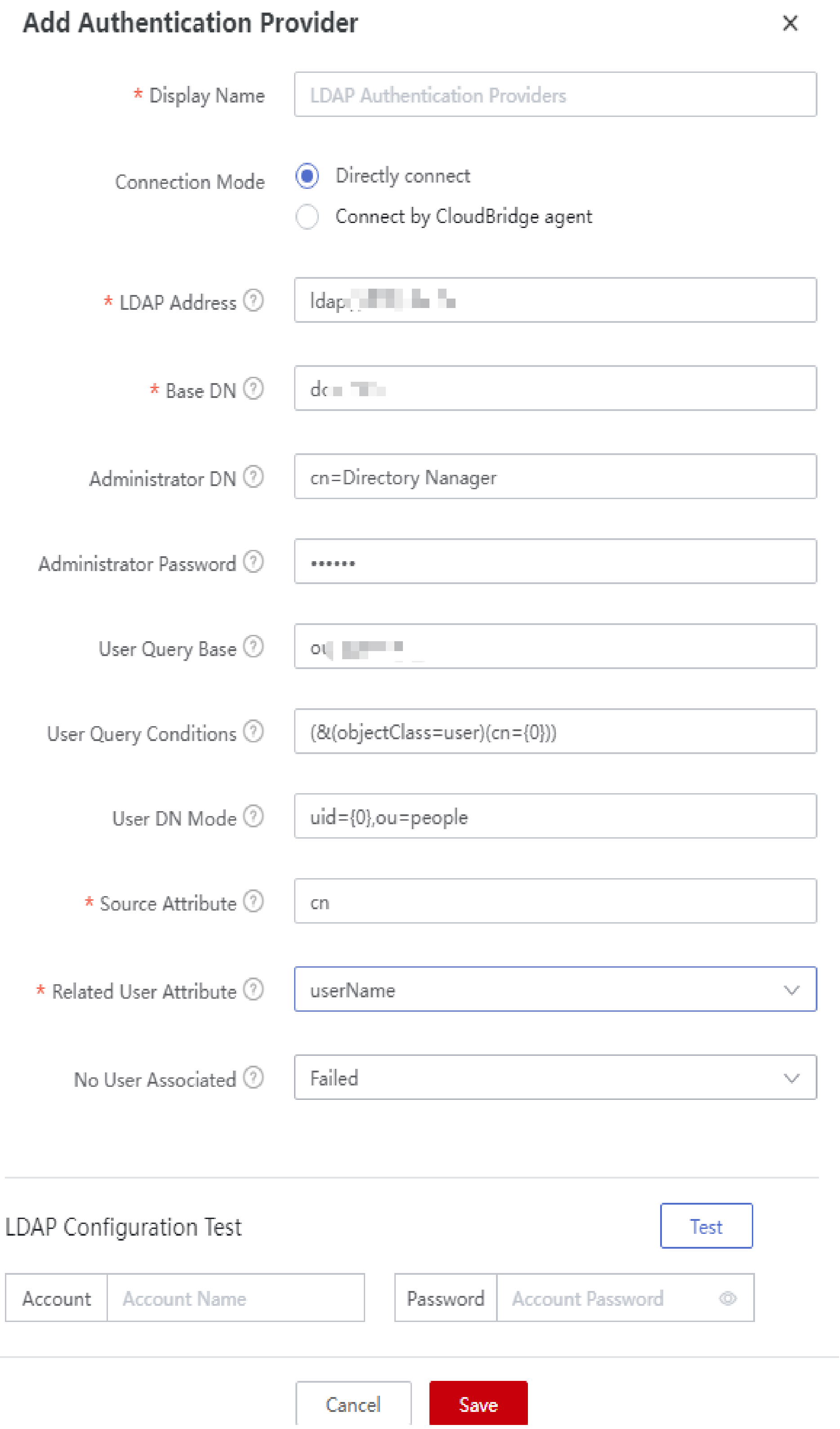
* Display Name	LDAP Authentication Providers
Connection Mode	● Directly connect ○ Connect by CloudBridge agent
* LDAP Address	Please enter the address and port of the LDAP server
* Base DN	dc=xxx,dc=xxx
Administrator DN	cn=Directory Manager
Administrator Password	Password of the administrator account in LDAP.
User Query Base	ou=people
User Query Conditions	(&(objectClass=user)(uid={0}))
User DN Mode	cn={0}
* Source Attribute	uid
* Related User Attribute	--Select--
No User Associated	Failed

LDAP Configuration Test

Account	Account Name	Password	Account Password

- 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.

Figure 5-24 Query authentication mode



Add Authentication Provider ×

* Display Name: LDAP Authentication Providers

Connection Mode: ● Directly connect ○ Connect by CloudBridge agent

* LDAP Address: ldap[redacted]

* Base DN: dc[redacted]

Administrator DN: cn=Directory Nanager

Administrator Password: ••••••

User Query Base: ou[redacted]

User Query Conditions: (&(objectClass=user)(cn={0}))

User DN Mode: uid={0},ou=people

* Source Attribute: cn

* Related User Attribute: userName

No User Associated: Failed

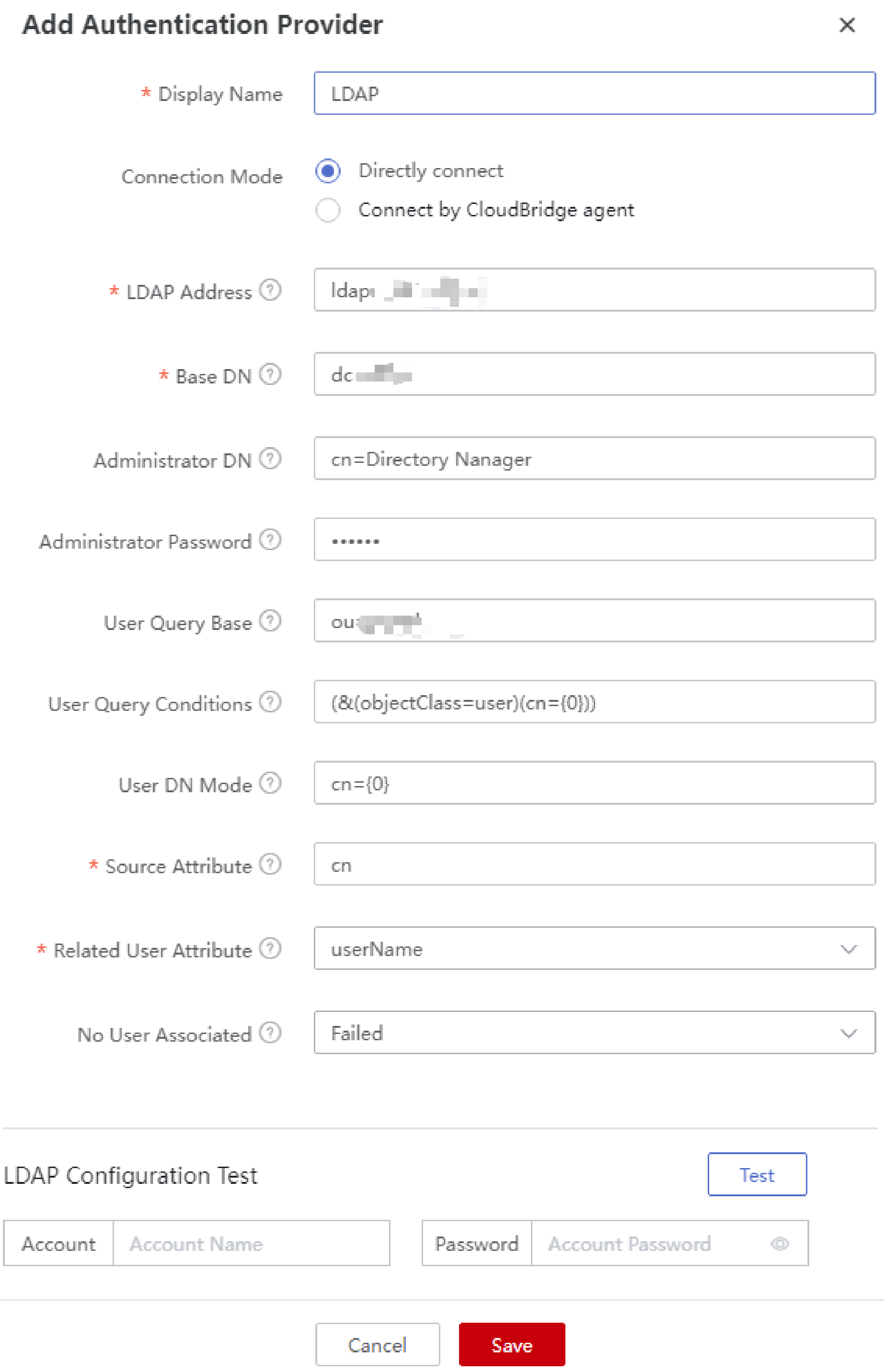
LDAP Configuration Test

Account: Account Name

Password: Account Password

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

Figure 5-25 DN and query authentication



Add Authentication Provider

* Display Name: LDAP

Connection Mode: ● Directly connect ○ Connect by CloudBridge agent

* LDAP Address: ldap[redacted]

* Base DN: dc[redacted]

Administrator DN: cn=Directory Nanager

Administrator Password: ••••••

User Query Base: ou[redacted]

User Query Conditions: (&(objectClass=user)(cn={0}))

User DN Mode: cn={0}

* Source Attribute: cn

* Related User Attribute: userName

No User Associated: Failed

LDAP Configuration Test

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

Step 1 Log in to the administrator portal.

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

Step 3 Choose **Enterprise Authentication Providers** > **LDAP**.

Step 4 On the **LDAP Authentication Providers** page, click **Add Authentication Provider** in the upper right corner and set the parameters required.

Table 5-14 Configuration parameters

Parameter	Mandatory	Description
Display Name	Yes	Custom 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**.
Base DN	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. You can select one from the drop-down list.
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 5-15**.

Table 5-15 Mapping parameters

Parameter	Description
User Attribute	Attribute in OneAccess that maps to LDAP.
Mapping Type	Mode of user attribute mapping between OneAccess and LDAP. **NOTE** ● If **Mapping Type** is set to **Authentication Provider Attribute**, **Source Attribute** is required. ● If **Mapping Type** is set to **Fixed Attribute Value**, **Fixed Attribute Value** is required. ● If **Mapping Type** is set to **Script-based**, **Script** is required.

----End

5.2.7.2 Configuring LDAP Authentication

Introduction

This section uses the OneAccess user portal as an example to describe how to configure the LDAP authentication function. After configuring the LDAP authentication provider in OneAccess, you can refer to this section to configure LDAP authentication for logging in to each application system.

Prerequisites

- You have permissions to access the administrator portal.
- You have configured the LDAP authentication provider in OneAccess by referring to **Configuring an LDAP Authentication Provider**.

Enabling LDAP Authentication

Step 1 Log in to the administrator portal.

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

Step 3 Click **User Portal** on the page.

Step 4 On the application information page, click the application icon.

Step 5 Choose **Login Settings** > **Web Applications**, click ○ in the **Operation** column of **LDAP** to enable LDAP authentication, and select the authentication provider added in **Adding an LDAP Authentication Provider**.

NOTE

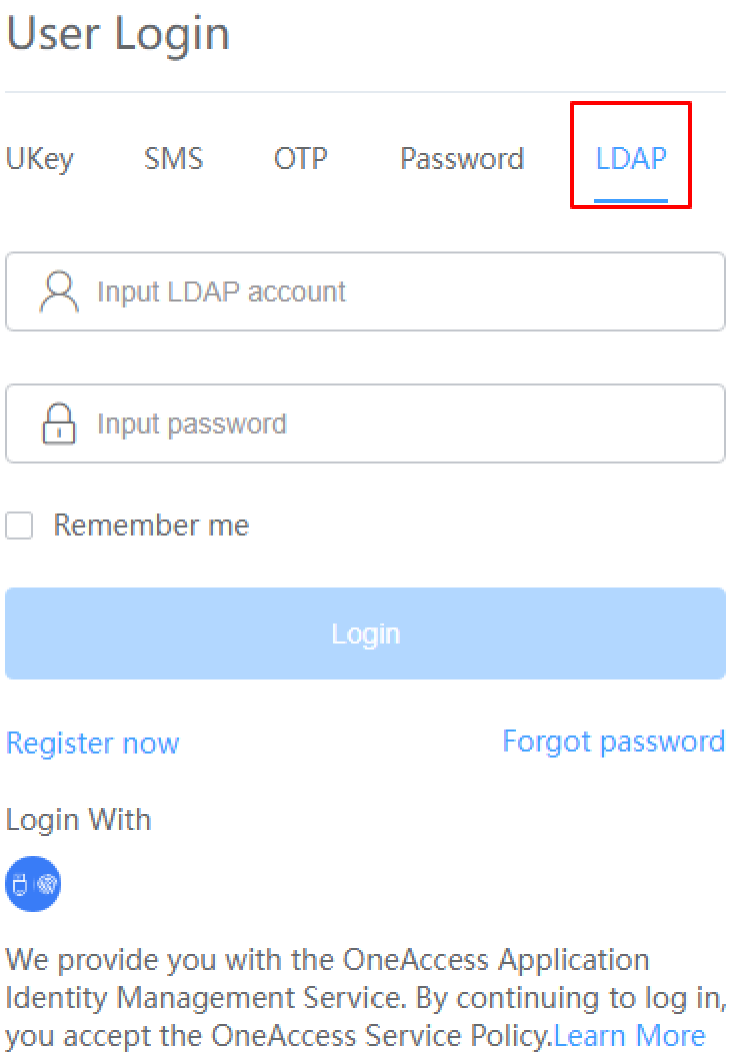
When LDAP authentication is enabled, the password login mode text box is used. You need to click in the **Operation** column of **Password** to disable the database authentication mode. If AD authentication is enabled, click in the **Operation** column of **AD** to disable AD authentication.

----End

Logging In to the User Portal Through LDAP Authentication

1. Go to the user portal login page, select **LDAP**, enter an LDAP account and password, and click **Login**.

Figure 5-26 Selecting LDAP



We provide you with the OneAccess Application Identity Management Service. By continuing to log in, you accept the OneAccess Service Policy.Learn More

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

NOTE

- To automatically create a user if the authorized user is not associated with any system user, set **No User Associated** to **Automatically create users**. For details, see **Table 5-14**.
- By default, users automatically created in the preceding scenario belong to the first root organization in the administrator portal.

6 Authorizing IAM Users to Access a OneAccess Instance Administrator Portal

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

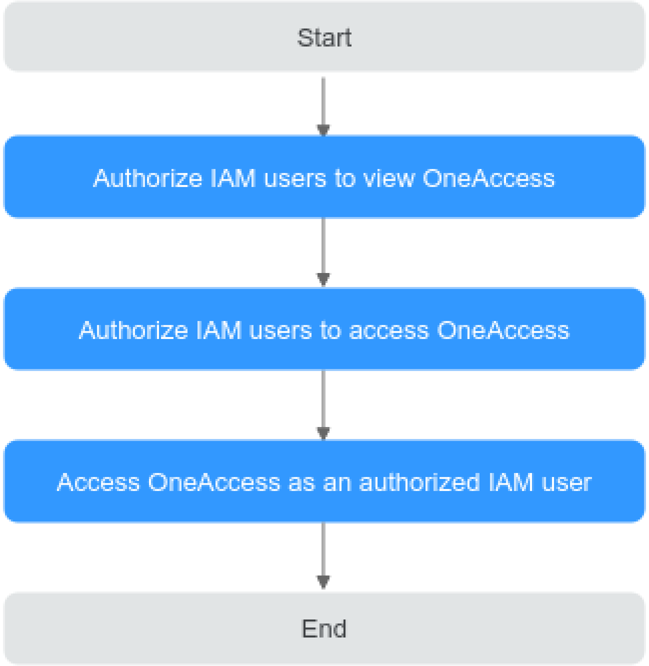
You can use your account to create IAM users and assign permissions for specific resources. Each IAM user has their own identity credentials (password and access keys) and uses cloud resources based on assigned permissions.

To log in to Huawei Cloud from OneAccess through SSO, see **Logging In to Single Huawei Cloud Account via OneAccess Without Password (SAML - Virtual User SSO)**.

IAM users can access OneAccess instances through Huawei Cloud. This helps the enterprise administrator to securely control access to OneAccess resources.

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

Configuration Process


Start
Authorize IAM users to view OneAccess
Authorize IAM users to access OneAccess
Access OneAccess as an authorized IAM user
End

Prerequisites

You have a Huawei Cloud account and have bought a OneAccess instance. For details about how to purchase such an instance, see **Buying an Instance**.

Authorizing IAM Users to View OneAccess

Create a user group on the IAM console, assign required permissions to the user group, create users, and add them to the user group. The users are thus authorized with the permissions of the user group.

Step 1 Create a user group on the IAM console and assign the **OneAccess ReadOnlyAccess** permission to the group. For details, see **Creating a User Group and Assigning Permissions**.

Step 2 Create a user on the IAM console and add the user to the group created in **Step 1**. For details, see **Creating an IAM User**.

Step 3 Log in to the console and verify the read-only permission by referring to **Logging In as an IAM User**.

----End

Authorizing IAM Users to Access OneAccess

Authorize IAM users to access OneAccess in the OneAccess console.

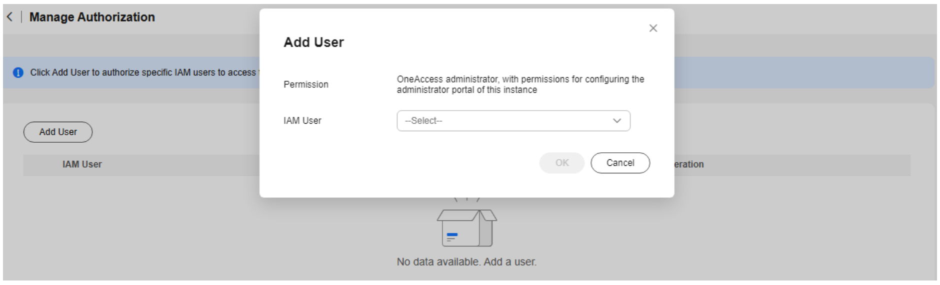
Step 1 Log in to the OneAccess console as an administrator.

Step 2 Click **Manage Authorization**.

Step 3 Click **Add User**, select the user created in **Step 2**, and click **OK** to authorize the IAM user to access OneAccess.

NOTE

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



< | **Manage Authorization**

Click Add User to authorize specific IAM users to access

Add User

IAM User	eration

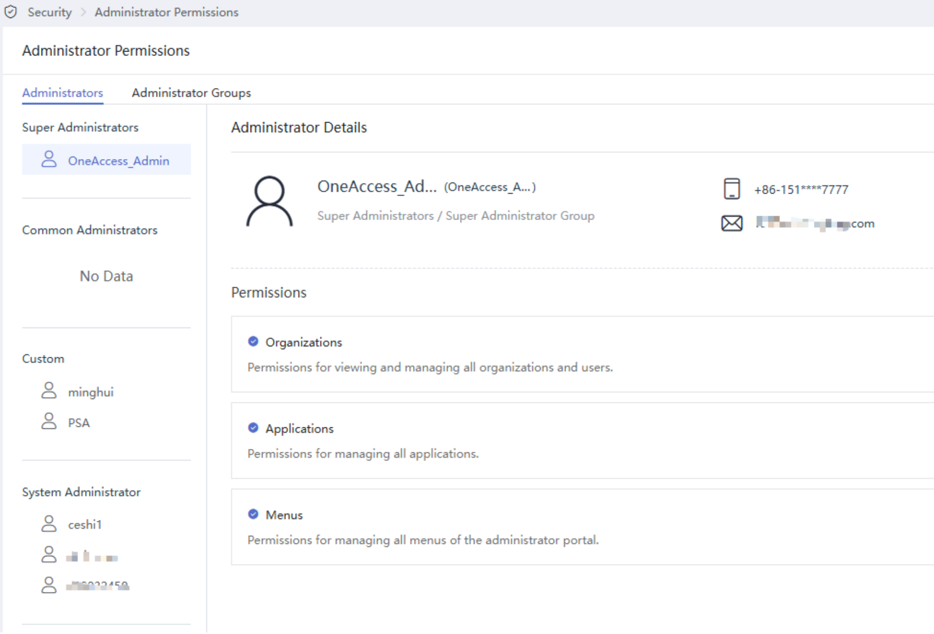
No data available. Add a user.

Add User

Permission: OneAccess administrator, with permissions for configuring the administrator portal of this instance

IAM User: --Select--

Step 4 Go to the administrator portal, and view the system administrator that is automatically generated.



Security > Administrator Permissions

Administrator Permissions

Super Administrators
- OneAccess_Admin

Common Administrators
- No Data

Custom
- minghui
- PSA

System Administrator
- ceshi1
- [redacted]
- [redacted]

Administrator Details

OneAccess_Ad... (OneAccess_A...)
Super Administrators / Super Administrator Group
+86-151****7777
[redacted]com

Permissions

Organizations
Permissions for viewing and managing all organizations and users.

Applications
Permissions for managing all applications.

Menus
Permissions for managing all menus of the administrator portal.

----End

Accessing OneAccess as an Authorized IAM User

Authorized IAM users can access the OneAccess administrator portal through Huawei Cloud.

Step 1 Log in to Huawei Cloud as an IAM user. For details, see **Logging In as an IAM User**. If you want to log in by scanning a QR code, refer to **Scanning QR Code to Log in**.

Step 2 Choose **Service List** > **Management & Governance** > **OneAccess**.

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 1**.

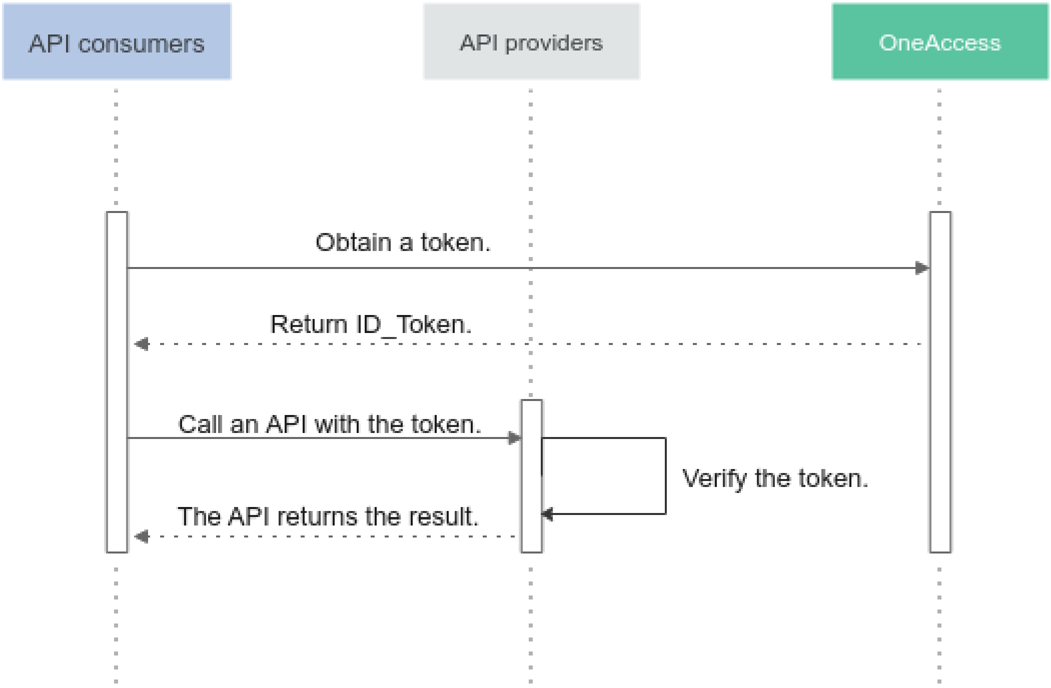
----End

7 API Usage

Overview

OneAccess provides a third-party API authorization management function. API providers configure APIs in OneAccess first. To use these APIs, API consumers obtain authentication tokens from OneAccess, and call the APIs with the authentication tokens. The API providers then determine whether to provide services to the API consumers based on the authentication tokens.

Figure 7-1 Overview



Prerequisite

You have permissions to access the administrator portal.

Adding an Application

Add applications to the administrator portal to provide authentication tokens to API consumers.

Step 1 Log in to the administrator portal.

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

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

Step 4 Obtain the client ID and client secret.

Click the application logo on the application information page, and obtain the values of **Client ID** and **Client Secret** on the application details page. (These values will be provided to API consumers.)

NOTE

- Click **Enable** to generate a client secret.
- Client secret is an important credential used to verify the identity of a developer. Do not provide the client secret to other developers nor store it in code.
- If you reset the client secret, the new client secret takes effect immediately, and all APIs that use the old client secret become invalid. Exercise caution when performing this operation.
- OneAccess does not store the client secret. Keep it properly after obtaining it.

----End

Adding an API

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

Step 1 Log in to the administrator portal.

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

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

Step 4 On the **Add Custom APIs** page, upload a product logo, enter the product name and description, and click **OK**.

Step 5 Click the created custom API, click the **Application Authorization** tab, and click **Authorize** next to the application added in Adding an Application to authorize the application to use the API.

Step 6 Click the **Permissions** tab and add API permissions.

----End

Granting API Permissions to an Application

Grant permissions for a specific custom API to applications.

Step 1 Log in to the administrator portal.

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

Step 3 Click the application added in **Adding an Application** and then click the logo of it. The **General Information** page is displayed.

Step 4 In the navigation pane, choose **API Permissions**. In the **Operation** column of a permission code, click **Authorize**.

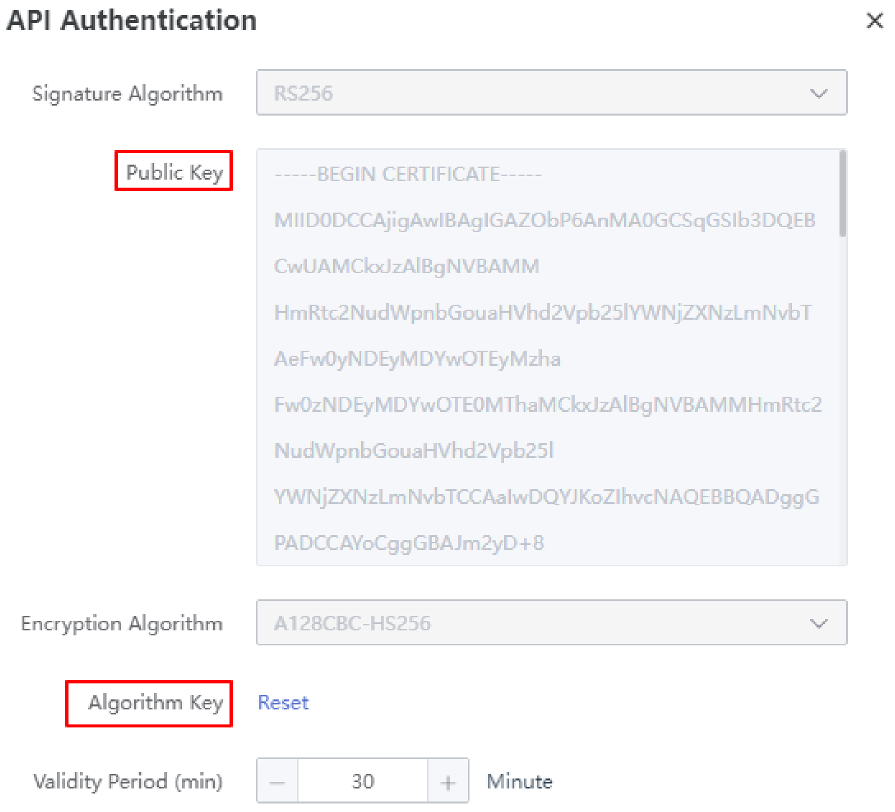
----End

Obtaining the Signature Public Key and Algorithm Key

The authentication tokens issued by OneAccess are encrypted and signed. Prepare the signature public key and algorithm key for the API provider to decrypt the token.

Step 1 Log in to the administrator portal.

Step 2 In the navigation pane, choose **Settings** > **Service Settings**. Click **API Authentication** to obtain the signature public key and algorithm key, and provide them for the API provider.



API Authentication

Signature Algorithm: RS256

Public Key:

```
-----BEGIN CERTIFICATE-----
MIID0DCCAjigAwIBAgIGAZObP6AnMA0GCSqGSIb3DQEB
CwUAMCkxJzAlBgNVBAMM
HmRtc2NudWpnbGouaHVhd2Vpb25lYWNjZXNzLmNvbT
AeFw0yNDEyMDYwOTEyMzha
Fw0zNDEyMDYwOTE0MThaMCkxJzAlBgNVBAMMHmRtc2
NudWpnbGouaHVhd2Vpb25l
YWNjZXNzLmNvbTCCAaIwDQYJKoZIhvcNAQEBBQADggG
PADCCAYoCggGBAJm2yD+8
```

Encryption Algorithm: A128CBC-HS256

Algorithm Key: Reset

Validity Period (min): – 30 + Minute

NOTE

OneAccess does not display the algorithm key. After resetting the algorithm key, keep it secure.

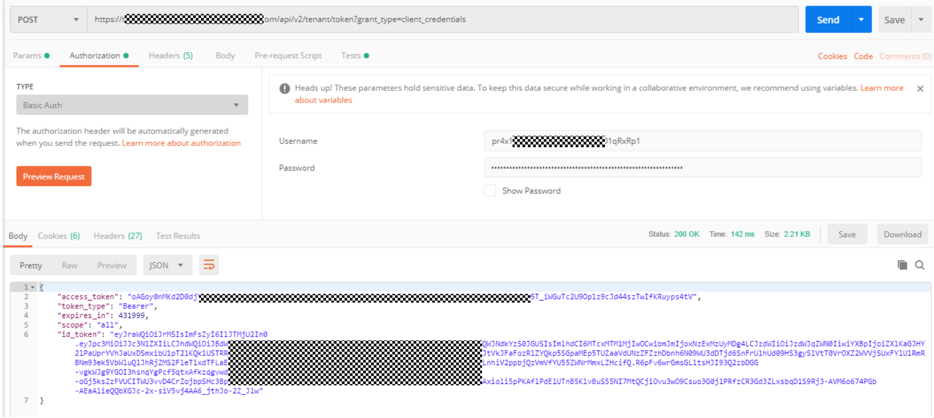
----End

(API Consumers) Obtaining an Authentication Token from OneAccess

API consumers obtain the authentication token by calling the OneAccess authentication API.

Access API: **https://***Access domain name***/api/v2/tenant/token?grant_type=client_credentials**

This is a Postman calling example.



POST https://[redacted]om/api/v2/tenant/token?grant_type=client_credentials

Authorization

TYPE: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables

Username: pr4x1[redacted]1qRxRp1

Password: ••

□ Show Password

Status: 200 OK Time: 142 ms Size: 2.21 KB

```
{
    "access_token": "oAGoy0nMKd2D0dj[redacted]5T_iWGuTc2U9Oplz9cJd44szTwIfKRuyps4tV",
    "token_type": "Bearer",
    "expires_in": 431999,
    "scope": "all",
    "id_token": "eyJraWQiOiJrMSIsImFsZyI6IlJTMjU2In0
        .eyJpc3MiOiJJc3N1ZXIiLCJhdWQiOiJBdW[redacted]QWJNdkYzS0JGUSIsImlhdCI6MTcxMTM1MjIwOCwibmJmIjoxNzExMzUyMDg4LCJzdWIiOiJzdWJqZWN0IiwiYXBpIjoiZXlKaGJHY
        21PaUprYVhJaUxDSmxibU1pT21KQk1USTRR          JtVkJFaFozRlZYQkp5SGpaMEp5TUZaaVdUNzZFZzhDbnh6N09WU3dDTjd6SnFrUlhUd09HS3gyS1VtT0VrOXZ2WVVjSUxFY1U1RmR
        BNm93ek5VbWluQlJhRjZMS2FleTlxdTFLaE          LnhiV2ppbjQzVmVfYU55ZWNrMmxLZHcifQ.R6pFv6wrGmsGLltsHJI93Q2zbDGG
        -vgkWJg9YGOI3hsnqYgPcf5qtxAfkzqgvwd
        -oGj5ksZzFVUCITWU3vvD4CrZojbpSHc3Bp          Axioli5pPKAflPdElUTnB5KlvBuS55NI7MtQCjiOvu3wO9Csuo3G0j1PRfzCR3Gd3ZLxsbqD1S9Rj3-AVM6o674PGb
        -AEaAlieQQbXGJc-2x-siV5vj4AA6_jthJo-2Z_Jlw"
}
```

NOTE

- Replace *Access domain name* with the real user access domain name. You can obtain it from the OneAccess instance details page.
- Set request method to **POST**, authentication type to **Basic Auth**, username and password to the values of **Client ID** and **Client Secret** obtained in **Step 4**, respectively.
- The returned **id_token** contains the signature information and the information for third-party API permission authorization. When the API consumers call the third-party API, they can send the value of **id_token** to the API provider for identity authentication and authorization. They can use header to send the information. The Authorization header is recommended.
- The returned **id_token** has a validity period, within which the value of **id_token** can be reused. The validity period is configured in the application.

(API Providers) Verifying a Token

After receiving an API request made by an API consumer with **id_token** obtained from OneAccess, the API provider needs to verify the token:

- Check whether the signature of the token is correct and whether the token is issued by OneAccess.
- Check whether the permissions declared in the token involve the current API.

Java code example:

```
import com.alibaba.fastjson.JSON;
import lombok.Data;
import org.apache.commons.codec.binary.Base64;
import org.jose4j.jwa.AlgorithmConstraints;
import org.jose4j.jwe.ContentEncryptionAlgorithmIdentifiers;
import org.jose4j.jwe.JsonWebEncryption;
import org.jose4j.jwe.KeyManagementAlgorithmIdentifiers;
import org.jose4j.jwk.JsonWebKey;
import org.jose4j.jwt.JwtClaims;
import org.jose4j.jwt.consumer.InvalidJwtException;
import org.jose4j.jwt.consumer.JwtConsumer;
import org.jose4j.jwt.consumer.JwtConsumerBuilder;
import org.jose4j.lang.JoseException;

import java.io.ByteArrayInputStream;
import java.io.InputStream;
import java.security.cert.CertificateException;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;
import java.security.interfaces.RSAPublicKey;
import java.util.HashMap;
import java.util.List;
import java.util.Map;

/**
 * @author : bsong
 **/
public class JWTTest {
    public static final String BEGIN_CERT = "-----BEGIN CERTIFICATE-----";
    public static final String END_CERT = "-----END CERTIFICATE-----";

    public static void main(String[] args) throws CertificateException, InvalidJwtException, JoseException {
        // The ID token is sent by the API caller
        String idToken = "";
        // Set the algorithm key in OneAccess
        String aesKey = "0123******************************************789abc";
        // Obtain the certificate from the administrator portal
        String certificate = "-----BEGIN CERTIFICATE-----\n" +
                "MIIC2jCCAcKgAwI.........................QEBCwUAMC4xLDAqBgNVBAMM\n" +
                "I2Jzb25nLmlkYWF.........................GUuY29tMB4XDTIyMDExNDA3\n" +
                "MDY1NVoXDTMyMDE.........................wwjYnNvbmcuaWRhYXMtdGVz\n" +
                "dC1hbHBoYS5iY2N.........................Ib3DQEBAQUAA4IBDwAwggEK\n" +
                "AoIBAQCJ7bfMCVX.........................GnE3W9uiSYk3WFkYFK8vh16\n" +
                "efVuvccAULE+xqi.........................652lsIBNOAC5YPy7J47z4iw\n" +
                "1GiAVYXxwyehgRe3.........................e0eJDKy6Ew5S+TUq72hqSD7\n" +
                "zrtQA3szqSK1pgFB.........................J8rMh9WiF2qUqzCdNRqkQRC\n" +
                "smGGj+PqD86otiif.........................0OPH5UOhR2OEve1cT9dgAlS\n" +
                "Vt1tKbE0l+iUTQqi.........................oZIhvcNAQELBQADggEBAEP8\n" +
                "EmkyoaWjngk3Tn5u.........................cJEDGTbuYO55wKap0BTetu6\n" +
                "cvGFxJYMQYefsx0.........................xn8N4ZgWvwgwDQVQx5WPgAT\n" +
                "QKunLWz30W4GYUE.........................QJZ7ift2sqoBLmkmjfcyqW0\n" +
                "jU1+7/e/ea5XAC3.........................DtVHqufwP4R/TALg1muaNyJ\n" +
                "f7obOcMHAb/OcbP.........................FSAwkVYsxSC9LEEUPhCONvX\n" +
                "KCWoeQoX/qkZH/nBvXU=\n" +
                "-----END CERTIFICATE-----";

        RSAPublicKey publicKey = getPublicKeyByCertificate(certificate);
        JsonWebKey jsonWebKey = getJsonWebKey(aesKey);
        JwtClaims jwtClaims = validateIDToken(publicKey, idToken);
        String apiPermission = jwtClaims.getClaimValue("api").toString();
        String permissionString = decryptionIDToken(jsonWebKey, apiPermission);
        System.out.println(permissionString);
        Map<String, List<String>> permissions = getPermissionsFromIdToken(permissionString);
        System.out.println(permissions);
    }

    public static Map<String, List<String>> getPermissionsFromIdToken(String permissionString) throws 
JoseException {
        Map<String, List<String>> result = new HashMap<>();
        Permission permission = JSON.parseObject(permissionString,Permission.class);
        permission.getAuz().stream().forEach(p ->{
            p.entrySet().forEach(e->{
                result.put(e.getKey(),e.getValue());
            });
        });
        return result;
    }

    @Data
    public static class Permission{
        List<Map<String, List<String>>> auth_method;
        List<Map<String, List<String>>> auz;
    }

    public static RSAPublicKey getPublicKeyByCertificate(String certificate) throws CertificateException {
        CertificateFactory fact = CertificateFactory.getInstance("X.509");
        byte[] decoded = Base64.decodeBase64(certificate.replace(BEGIN_CERT, "").replace(END_CERT, ""));
        InputStream input = new ByteArrayInputStream(decoded);
        X509Certificate cert = (X509Certificate) fact.generateCertificate(input);
        return (RSAPublicKey) cert.getPublicKey();
    }

    public static JsonWebKey getJsonWebKey(String key) throws JoseException {
        Map<String,Object> map = new HashMap<>();
        map.put("kty","oct");
        map.put("k",key);
        String jwkJson = JSON.toJSONString(map);
        return JsonWebKey.Factory.newJwk(jwkJson);
    }

    public static JwtClaims validateIDToken( RSAPublicKey publicKey,String idToken) throws
InvalidJwtException {
        JwtConsumer jwtConsumer = new JwtConsumerBuilder()
                .setRequireExpirationTime()                 // The JWT must have an expiration time
                .setAllowedClockSkewInSeconds(300)          // Allow some leeway in validating time-based
claims to account for clock skew
                .setRequireSubject()                        // The JWT must have a subject claim
                .setExpectedIssuer("Issuer")                // Whom the JWT needs to have been issued by
                .setExpectedAudience("Audience")            // Whom the JWT is intended for
                .setVerificationKey(publicKey)
                .build();
        return jwtConsumer.processToClaims(idToken);
    }

    public static String decryptionIDToken(JsonWebKey jwk, String idToken) throws JoseException {
        JsonWebEncryption jsonWebEncryption = new JsonWebEncryption();
        jsonWebEncryption.setAlgorithmConstraints(new
AlgorithmConstraints(AlgorithmConstraints.ConstraintType.PERMIT,
KeyManagementAlgorithmIdentifiers.DIRECT));
        jsonWebEncryption.setContentEncryptionAlgorithmConstraints(new
AlgorithmConstraints(AlgorithmConstraints.ConstraintType.PERMIT,
ContentEncryptionAlgorithmIdentifiers.AES_128_CBC_HMAC_SHA_256));
        jsonWebEncryption.setCompactSerialization(idToken);
        jsonWebEncryption.setKey(jwk.getKey());
        return jsonWebEncryption.getPlaintextString();
    }
}
```

8 Configuring MFA for User Login

OneAccess supports MFA during user login, which is more secure. This section uses the user portal as an example to describe how to configure and use MFA.

Prerequisite

You have permissions to access the administrator portal.

Enabling MFA

Enable and configure MFA for applications on the administrator portal.

Step 1 Log in to the administrator portal.

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

Step 3 On the application page, expand the **Pre-integrated Applications** section, and click the user portal logo.

Step 4 In the **Access Control** section, click ◯. On the page that is displayed, select MFA for **Default Policy**, set the authentication frequency and method, and click **Save**.

NOTE

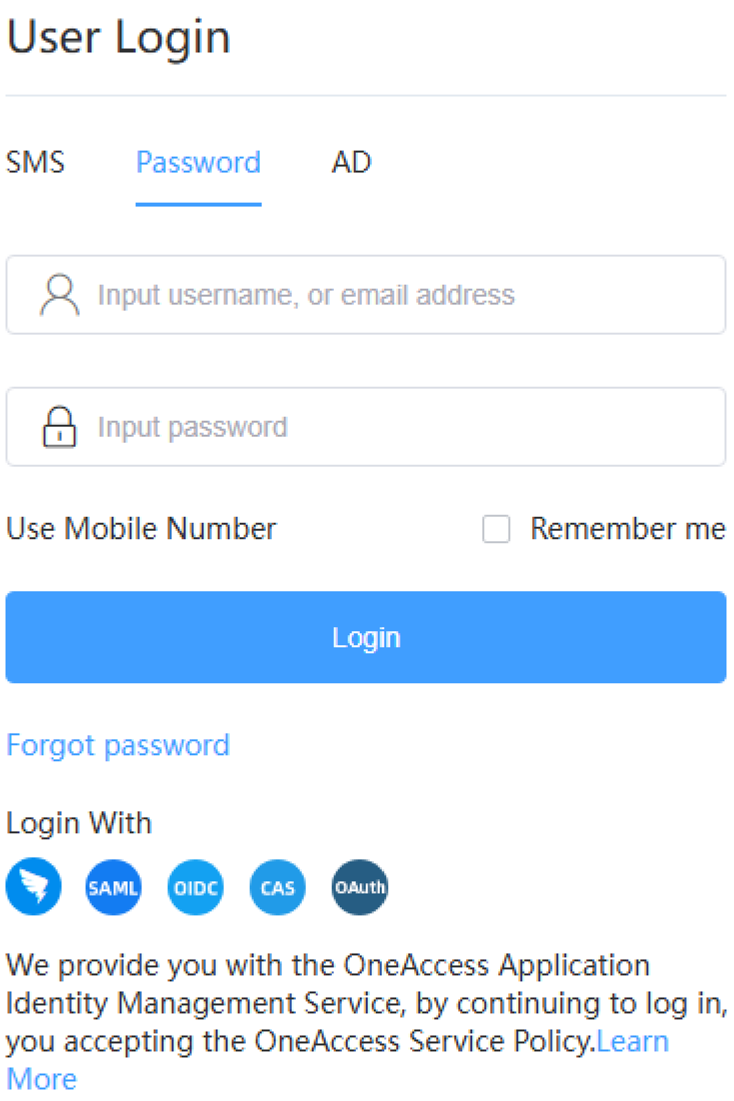
- Enable **Authentication** before you configure access control.
- If you select multiple MFA methods, users can select one of them when they log in to the system.
- If you select FIDO2, configure the FIDO authentication providers by referring to **Built-in Authentication Providers**.

Step 5 Click **Add Policy**. On the displayed page, configure the access control parameters and click **Save**. For details about the parameters, see **Access Control**.

----End

Accessing the User Portal

A user accesses the user portal. After the login is successful, the MFA page is displayed. After the authentication is successful, the user portal is displayed.



User Login

SMS Password AD

Input username, or email address

Input password

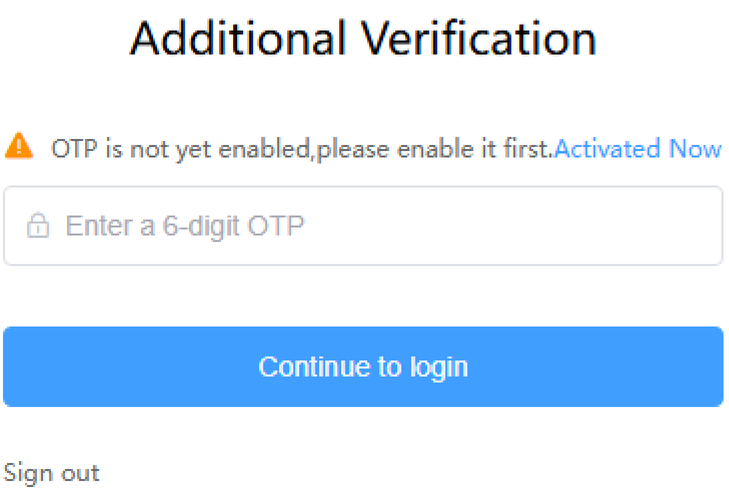
Use Mobile Number

□ Remember me

Forgot password

Login With

We provide you with the OneAccess Application Identity Management Service, by continuing to log in, you accepting the OneAccess Service Policy.Learn More



Additional Verification

OTP is not yet enabled,please enable it first.Activated Now

Enter a 6-digit OTP

Sign out