

OneAccess

Getting Started

Issue 01
Date 2024-12-26



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

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

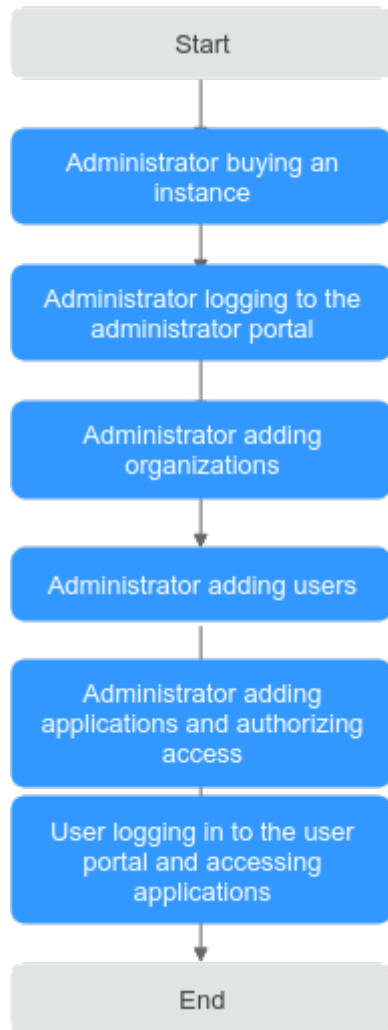
Contents

1 (Common User) Logging In to the User Portal and Accessing Applications.....	1
2 Common Practices.....	10

1 (Common User) Logging In to the User Portal and Accessing Applications

Figure 1-1 shows the general process of using OneAccess, which aims to provide you an overview of OneAccess basic operations. By performing the basic operations, as an administrator, you can configure and manage users and applications in the administrator portal and authorize the users to access specific applications in the user portal through single sign-on (SSO).

Figure 1-1 Basic operation process



1. Before using OneAccess, as an administrator, you need to purchase an instance by referring to [Buying an Instance](#).
2. After purchasing a OneAccess instance as an administrator, you can log in to the administrator portal of the instance by referring to [\(Administrator\) Logging to the Administrator Portal](#).
3. You can add an organization by referring to [\(Administrator\) Adding Organizations](#).
4. You can add users in the administrator portal by referring to [\(Administrator\) Adding Users](#).
5. OneAccess provides more than 1,000 pre-integrated applications. You can also add custom applications. For details about how to add applications and authorize access, see [\(Administrator\) Adding Applications and Authorizing Access](#).
6. You can access applications through the OneAccess user portal. For details, see [\(Common User\) Logging In to the User Portal and Accessing Applications](#).

Preparations

1. Register with Huawei Cloud and complete real-name authentication.
If you already have one, skip this step. If you do not have one, do as follows:
 - a. Log in to the [Huawei Cloud official website](#), and click **Register**.
 - b. Sign up for a HUAWEI ID. For details, see [Signing up for a HUAWEI ID and Enabling Huawei Cloud Services](#).
After your ID is created, the system redirects you to your personal information page.
 - c. Complete real-name authentication. For details, see [Individual Real-Name Authentication](#).

NOTE

Real-name authentication is required only when you buy or use resources in the Chinese mainland.

2. Top up your account.
Ensure enough balance in your account.
 - For details about the prices of OneAccess, see "OneAccess Pricing Details".
 - For details about top-up, see [Top-Up and Repayment](#).
3. Grant permissions.
Before creating a OneAccess instance and its dependencies, you need to obtain specific permissions. For details, see [Permissions Management](#).

Buying an Instance

Step 1 Go to the page for buying OneAccess.

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

1. Select a region from the **Region** drop-down list.
2. Select an instance specification. Currently, the basic, professional, and enterprise editions are supported. Basic edition is selected as an example here.
3. Set **Number of Users** to **100**.
4. Set **Required Duration**. **Auto-renew** is selected by default.
5. Set **Number of Instances** to an integer ranging from 1 to 100. Select **1** here.

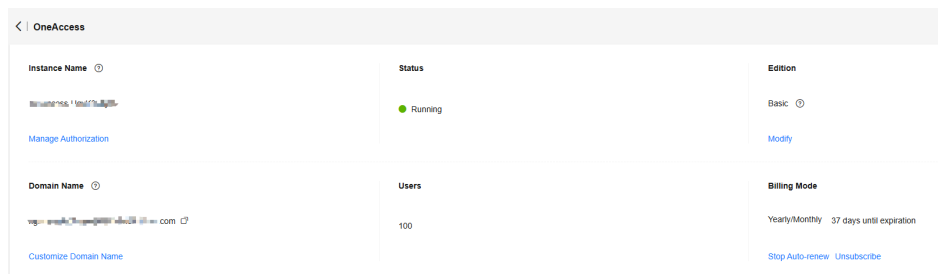
Step 3 Click **Next: Confirm**.

Step 4 Select **I have read and accepted <OneAccess Service Statement>** and click **Pay**.

----End

(Administrator) Logging to the Administrator Portal

1. Log in to the Huawei Cloud console.
2. Choose **Service List > Management & Governance > OneAccess**.
3. Click the OneAccess instance to be accessed.
4. Click the name of the instance to be accessed to go to the OneAccess instance administrator portal.



If you do not have permission to access the OneAccess instance, you need to access the OneAccess administrator portal as an IAM user and request access permission for the instance. For details, see [Creating an Authorization](#).

(Administrator) Adding Organizations

Organizations are used to manage enterprise employees. Each organization may represent a company or department and contains all employees in the company or department. As the root node, the top-level organization can have multiple sub-organizations and users. You can also add multiple levels of organizations and users under sub-organizations to manage employees of your enterprise.


- Step 1** Log in to the administrator portal.
- Step 2** In the top navigation pane, choose **Users > Organizations and Users**.
- Step 3** Click  in the lower left corner.
- Step 4** On the **Create Organization** page, specify organization parameters and click **OK**.

Table 1-1 Organization information

Parameter	Description
Organization Type	Type of an organization. The options are Department , Unit , Company , and Group .
Organization Code	Unique ID of the organization.
Organization Name	Organization name. Organizations at the same level must have different names.
Sequence	Position of the organization under the parent organization.
Parent Organization	Parent organization of the organization to be created. Leave this field blank when creating a top-level organization.

Step 5 Click **OK**.

----End

(Administrator) Adding Users


On the OneAccess administrator portal, you can create an organization for one user or create a user that belongs to multiple organizations. As an administrator, you can add users in the administrator portal. Users then use their own accounts to access specific applications.

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

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


Table 1-2 Basic information

Parameter	Description
Username	You can determine whether this is mandatory by referring to Modifying User Attributes . If the default username is used, the system automatically generates a username. You can set the character and length requirements of the username in Modifying User Attributes . The username of the user cannot be the same as those of other users. The username is case insensitive.

Parameter	Description
Organization	<p>You can specify an organization to which the user to be added belongs. You can select one or more organizations. By default, the first selected organization is the primary organization. For details about how to add an organization, see (Administrator) Adding Organizations.</p> <p>NOTE</p> <ul style="list-style-type: none"> If you select an organization in the organization tree on the left and then click Create User, the selected organization is the primary organization by default. A user can have up to one primary and nine secondary organizations. You can click  on the right of the target username and select Change Organization. In the displayed dialog box, adjust the primary/secondary organization.
Name	<p>You can set whether the attribute is mandatory and the length of it by referring to Modifying User Attributes.</p>
Cell phone number	<p>You can set whether the attribute is mandatory and the length of it by referring to Modifying User Attributes. This must be unique.</p>
Email	<p>You can set whether the attribute is mandatory and the length of it by referring to Modifying User Attributes. This must be unique.</p>
area	<p>Select the user's country or region. You can set whether the attribute is mandatory by referring to Modifying User Attributes.</p>
city	<p>Enter the city where the user is located. You can set whether the attribute is mandatory and the length of it by referring to Modifying User Attributes.</p>

 **NOTE**

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

Step 5 Click  to enable password login. There are two login modes. Select **Set now**.

- You can customize the user login password when selecting **Set now**.
 - If you select **Rest password at first login**, you need to change the login password when you log in to the user portal for the first time.
 - If you do not select **Rest password at first login**, you do not need to change the password for your first login.
- **Automatically generated:** A password is automatically generated. The system notifies the user of the initial password and the user must log in to the system within the validity period. If the password initialization function is not enabled, configure it by referring to [Password Initialization Settings](#).

Step 6 Click **OK**.

----End

(Administrator) Adding Applications and Authorizing Access

The following procedure describes how to add an application using SAML. For details about how to add applications using other protocols, see [Application Integration](#).

Step 1 Log in to the administrator portal.

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

Step 3 On the **Pre-integrated Applications** page, click **Add Pre-integrated Application**.

Step 4 On the **Add Pre-integrated Application** page, select the application you want to add.

Step 5 On the **Add Application** page, set the basic information.

Table 1-3 General information

Parameter	Description
Logo	Upload a logo image of the application that does not exceed 50 KB.
Name	Name of the application. This field is required.

Parameter	Description
Authentication Method	Authentication mode of the application. This field cannot be changed.
Synchronization Method	Synchronization mode of the application. This field cannot be changed.

Step 6 Click **Next** and import the metadata of the application.

 **NOTE**

- You can import or enter the metadata of a pre-integrated application. To ensure accuracy of the metadata, you are advised to import the metadata file.
- The metadata needs to be obtained from the enterprise application.

Step 7 After the configuration is complete, click **Next**.

Step 8 Click an application. The **Application Information** page is displayed.

Step 9 On the displayed page, click  next to **Application Organization** in the **Object Models** area. In the displayed dialog box, click **OK**.

Step 10 On the **Application Information** page, click **Authorize** next to **Application Organizations** in the **Authorization** area.

Step 11 Click **Authorization Policy**.

Step 12 Click  to enable **Automatic Organization Authorization** and select **Custom**.

Step 13 Select the desired organizations, click **Save**, and then click **Add**.

Step 14 In the navigation pane, choose **Authorization > Application Accounts**.

Step 15 Click **add Accounts**.

Step 16 Select the users in **(Administrator) Adding Users**, authorize them to access the application, and click **Save**.

 **NOTE**

After authorization, accounts are automatically created for the users to access the application.

----End

(Common User) Logging In to the User Portal and Accessing Applications

To log in to the user portal and access applications, do as follows:

Step 1 Obtain the user portal domain name from the administrator.

 **NOTE**

A user access domain name is automatically generated after the administrator purchases a OneAccess instance. The domain name is displayed on the instance details page of the OneAccess console. For or example, **example.huaweioneaccess.com**.

Step 2 Visit the user access domain name.

Step 3 Enter the username and password and click **Log In**.

Step 4 Click the application added in [\(Administrator\) Adding Applications and Authorizing Access](#) to access it.

----End

2 Common Practices

After purchasing a OneAccess instance, you can perform operations based on your service requirements.

Practice		Description
Identity source integration	Integrating AD	This practice describes how to configure an AD identity source in OneAccess, allowing you to import and synchronize user and organization information in real time.
	Integrating LDAP	This practice describes how to configure an LDAP identity source in OneAccess, allowing you to import and synchronize user and organization information in real time.
Application integration	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	This practice describes how to integrate an application with OneAccess using SAML.
	SSO Access to Applications Through OAuth2.0	This practice describes how to integrate an application with OneAccess using OAuth.
	SSO Access to Applications Through OIDC	This practice describes how to integrate an application with OneAccess using OIDC.
	SSO Access to Applications Through CAS	This practice describes how to integrate an application with OneAccess using CAS.
	SSO Access to Applications Through Plug-in Autocompletion	This practice describes how to integrate an application with OneAccess using plug-in autocompletion.
Data synchronization	Synchronizing Data to Atlassian Through SCIM	This practice describes how to synchronize user data to Atlassian using SCIM.
	Synchronizing Data Through LDAP	This practice describes how to synchronize organization and user data to OpenLDAP using LDAP.
Authentication provider integration	Built-in Authentication Provider	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	This practice describes how to add a SAML authentication provider and configure SAML authentication login for applications on OneAccess.

Practice		Description
	OIDC Authentication	This practice describes how to add a OIDC authentication provider and configure OIDC authentication login for applications on OneAccess.
	CAS Authentication	This practice describes how to add a CAS authentication provider and configure CAS authentication login for applications on OneAccess.
	OAuth Authentication	This practice describes how to configure an OAuth authentication provider and configure OAuth authentication login for applications on OneAccess.
	Kerberos Authentication	This practice describes how to configure a Kerberos authentication provider and configure Kerberos authentication login for applications on OneAccess.
	AD Authentication	This practice describes how to configure an AD authentication provider and configure AD authentication login for applications on OneAccess.
	LDAP Authentication	This practice describes how to configure an LDAP authentication provider and configure LDAP authentication login for applications on OneAccess.