OneAccess

Service Overview

Issue	01
Date	2024-12-26

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

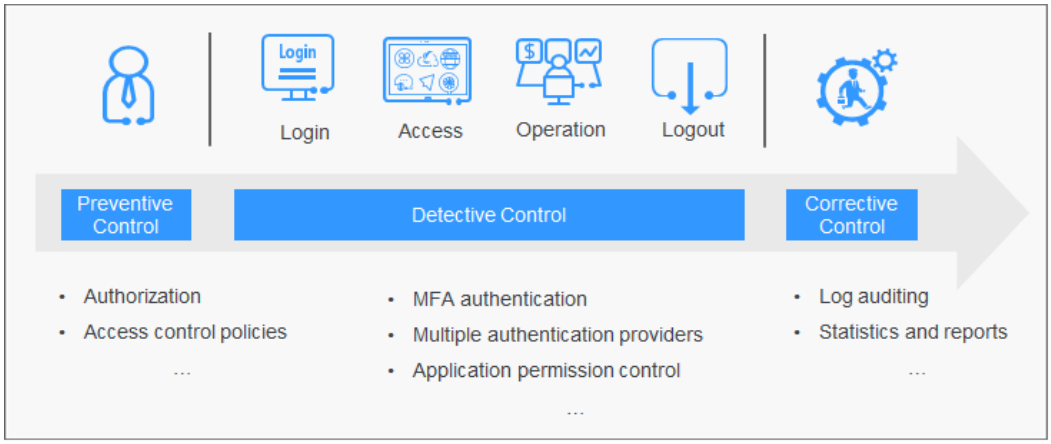
1 What Is OneAccess

OneAccess is an identity management service that enables you to centrally manage, authenticate, and authorize identities. With OneAccess, you can control access of your users to cloud and on-premises systems, and defend against access risks.

NOTE

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

Figure 1-1 OneAccess



Functions

- **Unified identity management**

  Manage organizations, users, user groups, applications, accounts, and credentials, synchronize identity data from identity sources to specific applications, access applications through a self-service user portal, and configure a password policy to improve account security.

- **Unified permissions management**

  Manage permissions required for accessing OneAccess and applications by using different authorization methods and permissions.

- **Unified authentication**

  Use multiple authentication modes, authentication policies, access control, single sign-on (SSO), and single logout (SLO) to facilitate trusted identity authentication and improve information security.

- **Intelligent access control**

  Use preset rules to identify risks during user access based on the access time, location, device, and user behavior, and automatically adjust the authentication method if a risk is identified.

- **Process audit**

  Query, track, and audit authentication, access, operation, synchronization, and system logs.

Advantages

- **Efficient enterprise management**
  - Store full lifecycle user accounts and data, and centrally manage user information and application accounts.
  - Automatically create accounts, modify permissions, and disable and delete accounts throughout the employee lifecycle, covering onboarding, job transfer, and resignation.
  - Integrate your local identity system and individual/enterprise social identity sources with OneAccess to synchronize organization and identity data, making full use of existing data assets and improving user login experience.
- **SSO access**
  - Access applications using the same account and URL through a unified portal.
  - OneAccess pre-integrates with more than 1,000 third-party applications. Users can access applications that they are authorized to access, without providing a password.
  - Connect to different data sources through multiple protocols, including Central Authentication Service (CAS), Security Assertion Markup Language 2.0 (SAML 2.0), OAuth 2.0, and OpenID Connect (OIDC).
  - Secure access through multiple authentication modes, including static password, SMS, QR code scanning, and one-time password (OTP). You can combine different authentication modes to suit your requirements.
- **High resource security**
  - Monitor user access behavior, including time, places, and devices, based on preset risk management rules to detect potential risks.
  - Eliminate potential risks and notify administrators and users of the risks based on conditional access control policies.
  - Customize access control policies by combining multiple environment factors including time, place, and device, and block access or require users to perform multi-factor authentication (MFA) in case a risk is detected.
- **Low O&M costs**
  - OneAccess pre-integrates more than 1,000 applications, which are available out-of-the-box. You do not need to construct the same

applications and can avoid indirect loss caused by information security incidents.

– Buy specifications as required.

Access Methods

You can access OneAccess using either of the following methods:

- Management console

  Access OneAccess through the management console — a browser-based visual interface.

- REST APIs

  Access OneAccess using REST APIs in a programmable way.

2 Concepts

Enterprise Administrator

Enterprise administrators include the account administrator and users who have administrator permissions for OneAccess. Enterprise administrators manage users, user groups, organizations, applications, and APIs in the administrator portal.

Super Administrator

The account administrator can create super administrators in the administrator portal to manage all organizations, users, and applications in your enterprise. Super administrators belong to the super administrator group, which has full access to the administrator portal.

Common Administrator

The account administrator or super administrators can create common administrators in the administrator portal to manage specific organizations, users, and applications in your enterprise. Common administrators do not belong to any group or belong to a common administrator group that only has permissions for specific menus of the administrator portal.

System Administrator

System administrators are created by Huawei Cloud master accounts in Identity and Access Management (IAM). They can access the organizations, users, and applications menus in the administrator portal but cannot create administrators. System administrators do not belong to any management group.

User

Users include employees, partners, and customers who use enterprise applications. They can log in to the user portal to access applications.

Application

Applications are third-party systems that you can manage and authorize access in OneAccess. There are pre-integrated and custom applications.

- Pre-integrated applications: Pre-integrated with OneAccess using development interfaces or protocols. You can use these applications only after purchasing them and completing basic configurations.
- Custom applications: In-house developed applications or software and commercial applications that are not included in the pre-integrated application list. To use custom applications, integrate them using supported authentication protocols and synchronization methods.

Identity Source

OneAccess allows you to import user and organization information from different systems and aggregate the information into a complete user directory for unified management. These systems are called identity sources. For example, AD, WeCom, DingTalk, Lark, XinRenXinShi, Beisen, MCHR, SAP SuccessFactors, Weaver e-cology9.0, and LDAP.

Authentication Provider

Users can log in to OneAccess using accounts and passwords of third-party systems. You can use CAS, SAML 2.0, OAuth 2.0, and OIDC, or add authentication providers, such as WeChat, Weibo, DingTalk, and WeCom.

SSO

SSO is an authentication scheme that allows users to log in with a single account and password to any applications that the users have been authorized to access, from the user portal. For example, after you add Huawei Cloud in the administrator portal and authorize access to a user, the user can log in to the user portal and access Huawei Cloud without entering their account and password again.

Open API Platform (OAP)

OAP is an open API provided by OneAccess for third-party developers to customize functions, such as management of organizations, users, and applications.

3 Edition Differences

OneAccess provides Basic, Professional, and Enterprise editions. **Table 3-1** describes the features supported by each edition.

- **Basic**: Provides basic functions with a quota of 100 or 500 users and supports yearly/monthly billing. It is suitable for small enterprises.
- **Professional**: Provides advanced functions (access control, permissions management, and capacity expansion) in addition to basic ones. The number of users can be 200 or 1,000 to 10,000. It meets high cost-effectiveness and reliability requirements of government organizations and medium and large enterprises. Yearly/month billing is supported.
- **Enterprise**: Provides independent resource deployment and advanced functions (access control and permissions management). It supports a maximum of 40,000 users and yearly/monthly billing, meeting the service requirements of large enterprises and governments.

Table 3-1 Features

Feature	Basic	Professional	Enterprise
Capacity expansion	Supported	Supported	Not supported
Conditional access control	Not supported	Supported	Supported
Custom API access control	Not supported	Supported	Supported
Fine-grained permissions	Not supported	Supported	Supported
Identity synchronization	Not supported	Supported	Supported
CloudBridge agents	Not supported	Supported	Supported
Organizations and users	Supported	Supported	Supported

Feature	Basic	Professional	Enterprise
Custom user attributes	Supported	Supported	Supported
Authentication via OAuth 2.0, SAML, OIDC, CAS, plug-in autofill, or OpenAPI	Plug-in autofill and OpenAPI are not supported.	Supported	Supported
Identity sources (WeCom, DingTalk, Lark, AD, LDAP, XinRenXinShi, Beisen, MCHR, SAP SuccessFactors, and Weaver e-cology9.0)	Supported	Supported	Supported
Manual and automatic application authorization	Supported	Supported	Supported
Internal and custom APIs	Custom APIs are not supported.	Supported	Supported
Authentication provider	WeChat, Weibo, QQ, Alipay, DingTalk, WeLink, WeCom, Cloud Hub, Lark, eteams, AD, and LDAP	WeChat, Weibo, QQ, Alipay, DingTalk, WeLink, WeCom, Cloud Hub, Lark, eteams, SAML, OIDC, OAuth, CAS, AD, LDAP, Kerberos, and FIDO2	WeChat, Weibo, QQ, Alipay, DingTalk, WeLink, WeCom, Cloud Hub, Lark, eteams, SAML, OIDC, OAuth, CAS, AD, LDAP, Kerberos, and FIDO2
Regions	Not supported	Supported	Supported
Administrator permissions	Supported	Supported	Supported
Password policy	Supported	Supported	Supported
Audit	Supported	Supported	Supported
Enterprise information	Supported	Supported	Supported
SMS gateway	Supported	Supported	Supported
Email gateway	Supported	Supported	Supported

Feature	Basic	Professional	Enterprise
DingTalk gateway	Supported	Supported	Supported
Voice gateway	Supported	Supported	Supported
Dictionaries	Supported	Supported	Supported
Data import	Supported	Supported	Supported
Entire parameter settings	Supported	Supported	Supported
Built-in and custom UI templates	Supported	Supported	Supported
Service configuration	Supported	Supported	Supported

4 Permissions Management

You can create users or administrators in OneAccess and grant them permissions for controlling access to specific applications or specific functions of the administrator portal. For details, see **(User) Logging In to the User Portal and Accessing Applications**.

If you need to assign different permissions for OneAccess instances you purchased on Huawei Cloud to employees in your organization, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your resources. You can use IAM to manage permissions for modifying OneAccess instances on Huawei Cloud.

You can create IAM users for your employees on your Huawei Cloud account, and assign permissions to these users on a principle of least privilege (PoLP) basis to control their access to specific resource types. For example, you can grant permissions to allow certain IT personnel in your enterprise to view OneAccess instances but disallow them to modify the certificates.

If your account does not require individual IAM users for permissions management, skip this section.

IAM is a free service of Huawei Cloud. You only pay for the resources in your account. For more information about IAM, see **What Is IAM?**

OneAccess Console Permissions

By default, new IAM users do not have permissions. To assign permissions to new users, you need to add them to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which you add them and can perform specific operations on cloud services.

OneAccess is a global service deployed and accessed without specifying any physical region. You can assign OneAccess permissions to users in the global service project. The users do not need to switch regions when they access OneAccess.

You can grant permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines service-level permissions based on user responsibilities. There are only a limited

number of roles for granting permissions to users. Huawei Cloud services depend on each other. When using roles to grant permissions, you also need to assign dependency roles. Roles are not an ideal choice for fine-grained authorization and secure access control.

- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization and secure access control. Most policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by OneAccess, see **OneAccess Actions**.

Table 4-1 lists all system-defined permissions for the OneAccess console.

Table 4-1 OneAccess console permissions

Role/Policy Name	Description	Type
Tenant Administrator	Permissions for all services except IAM, including all permissions for OneAccess.	System-defined role
Tenant Guest	Read-only permissions for all services except IAM. IAM users granted these permissions can only view this service and cannot configure resources in it.	System-defined role
IAM ReadOnlyAccess	Read-only permissions for IAM.	System-defined policy
OneAccess FullAccess	Full permissions for OneAccess.	System-defined policy
OneAccess ReadOnlyAccess	Read-only permissions for OneAccess. Users granted these permissions can only view this service and cannot configure resources in it.	System-defined policy

NOTE

Huawei Cloud accounts, authorized member accounts, and delegated accounts can purchase OneAccess instances. These accounts can use OneAccess only after instances are authorized.

Table 4-2 lists the common operations supported by system-defined permissions for OneAccess.

Table 4-2 Common operations supported by each system-defined policy or role of OneAccess

Operation	Tenant Administrator	Tenant Guest	OneAccess FullAccess	OneAccess ReadOnlyAccess
Querying instances	√	√	√	√
Querying domain certificate details	√	√	√	√
Ordering an instance	√ **NOTE** Member accounts and delegated accounts must have the IAM ReadOnlyAccess permission.	×	√ **NOTE** Member accounts and delegated accounts must have the IAM ReadOnlyAccess permission.	×
Customizing domain names	√	×	√	×
Unbinding custom domain names	√	×	√	×
Modifying domain certificates	√	×	√	×
Deleting an instance	√	×	√	×

OneAccess Actions

OneAccess provides system-defined policies, which can be directly used in IAM. You can also create custom policies to supplement system-defined policies for more refined access control. Operations supported by policies are specific to APIs. The following are basic concepts related to policies:

- Permissions: Statements in a policy that allow or deny certain operations.
- Actions: Specific operations that are allowed or denied.
- IAM or enterprise projects: Type of projects for which permissions can be granted. For example, policies that contain actions for both IAM projects and enterprise projects can be assigned in both IAM and Enterprise Management, but policies that contain only actions for IAM projects can be assigned only in IAM. For details about the differences between IAM and enterprise projects,

see **What Are the Differences Between IAM Projects and Enterprise Projects?**

Permission	Action	IAM Project	Enterprise Project
Enabling product instances	oneaccess:instances:create	√	×
Querying instances	oneaccess:instances:get	√	×
Customizing domain names	oneaccess:domains:create	√	×
Unbinding custom domain names	oneaccess:domains:delete	√	×
Querying domain certificate details	oneaccess:certificates:get	√	×
Modifying domain certificates	oneaccess:certificates:update	√	×
Modifying specifications	oneaccess:instances:update	√	×
Granting user permissions for specific instances	oneaccess:permissions:grantRoleToUser	√	×
Removing permissions granted to users for specific instances	oneaccess:permissions:revokeRoleFromUser	√	×
Querying permissions	oneaccess:permissions:listRoles	√	×
Querying permissions of authorized users	oneaccess:permissions:listRolesForUser	√	×
Querying authorized users of an instance	oneaccess:permissions:listUsersOnInstance	√	×

