

IAM Identity Center

Service Overview

Issue 01
Date 2023-08-30



Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Contents

1 What Is IAM Identity Center?	1
2 Application Scenarios	3
3 Functions	6
4 Permissions	7
5 Notes and Constraints	10
6 Billing	12
7 Concepts	13
8 Change History	14

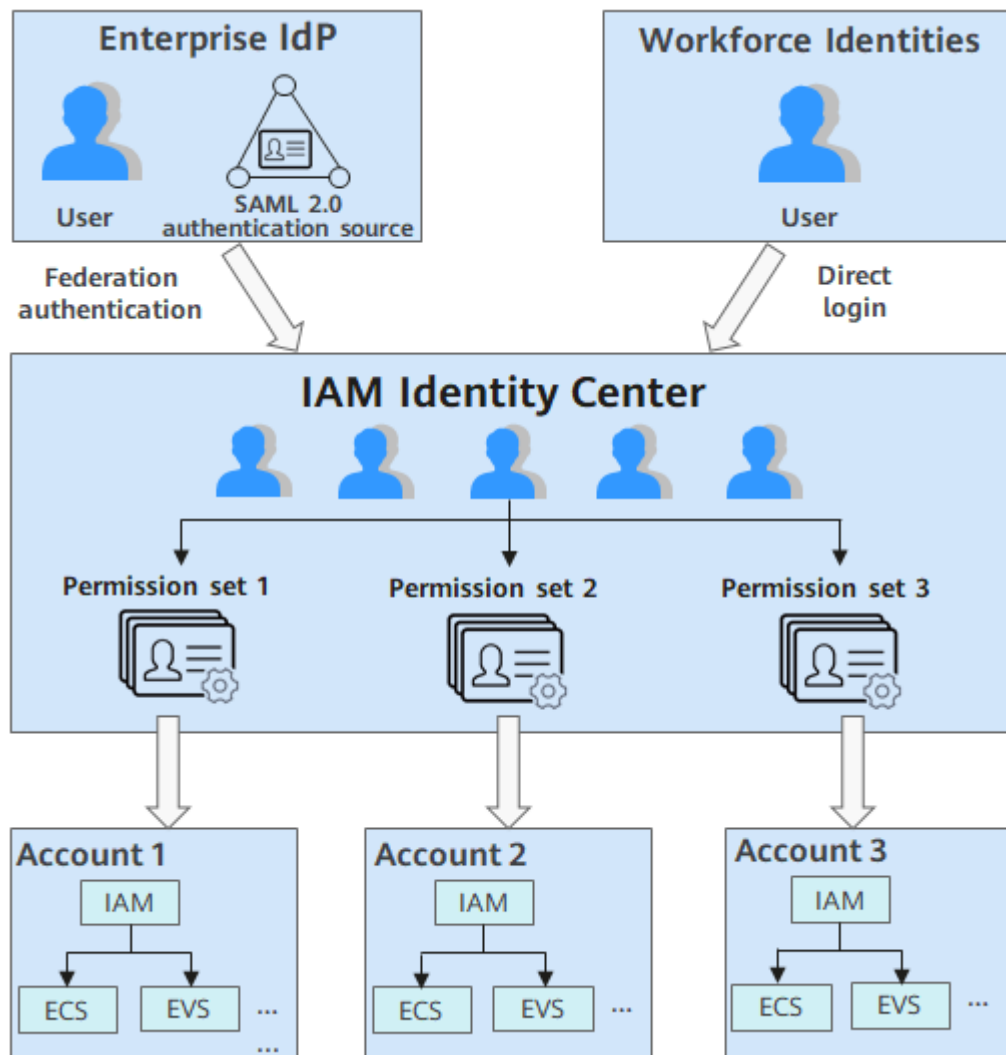
1 What Is IAM Identity Center?

Introduction

IAM Identity Center helps you centrally manage your workforce identities and their access to multiple Huawei Cloud accounts. You can create identities for your entire enterprise at one go and give them single sign-on (SSO) access with managed permissions. The IAM Identity Center administrator creates users, assigns passwords, and manages users by group. A single portal provides users with password-based SSO access to multiple accounts. A user who has passed the security verification in an application can access protected resources in other applications without logging in again.


Architecture

Figure 1-1 IAM Identity Center architecture



Access Methods

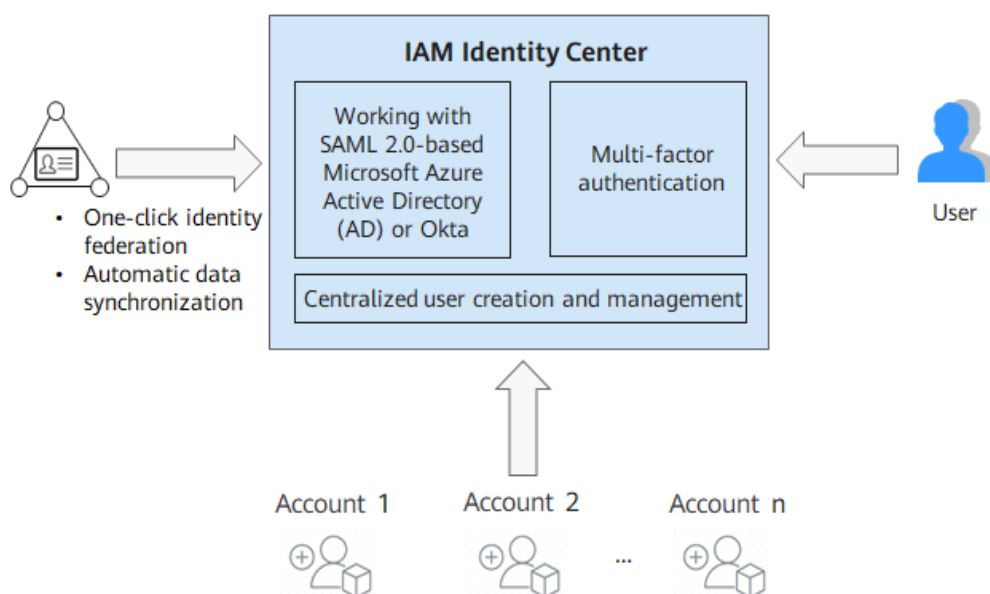
You can access the IAM Identity Center service through the management console or by calling HTTPS-based APIs.

- Accessing IAM Identity Center through the management console
The management console is a web-based GUI where you can easily perform various operations. Log in to the [management console](#). Click  in the upper left corner of the page and choose **Management & Governance > IAM Identity Center**.
- Accessing IAM Identity Center through APIs
Use this access method if you are required to integrate IAM Identity Center on Huawei Cloud into a third-party system for secondary development. For detailed operations, see the [IAM Identity Center API Reference](#).

2 Application Scenarios

Centralized Identity Management: Enabling Secure Access to Multiple Accounts Through One-Time Configuration

Figure 2-1 Centralized identity management



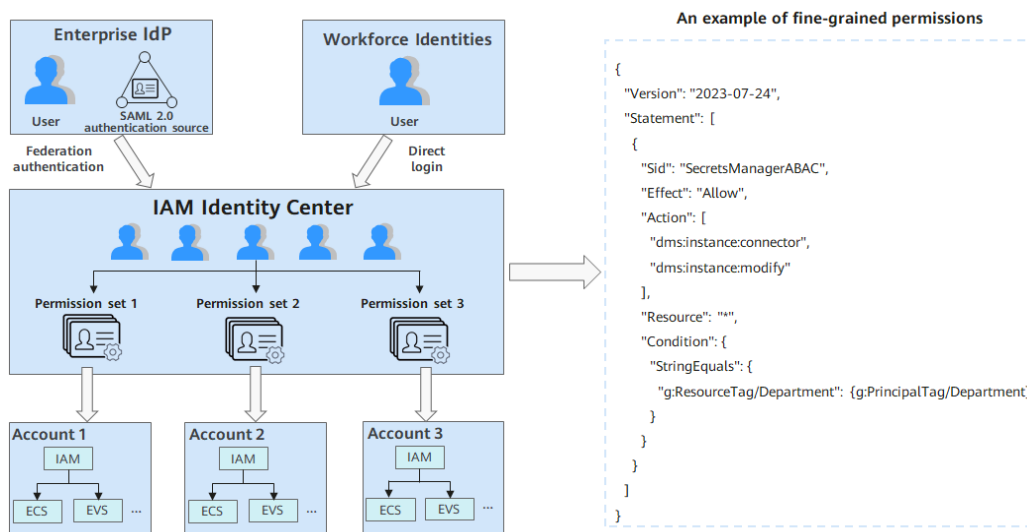
If an enterprise has multiple Huawei Cloud accounts and their workforce users need to access resources under multiple accounts, they have to log in to those accounts individually or create IAM users under the accounts, causing high maintenance costs and low efficiency. In this scenario, IAM Identity Center has the following advantages:

- Centralized user creation and management
 - The IAM Identity Center administrator creates users, assigns passwords, and manages users by group. A single portal provides users with password-based SSO access to multiple accounts.
- Seamless working with identity systems

- IAM Identity Center works with SAML 2.0-based Microsoft Azure Active Directory (AD) or Okta.
- IAM Identity Center automatically provisions users from SCIM-compliant identity providers. The IAM Identity Center administrator can manage users in Microsoft Azure AD or Okta. User information is automatically synchronized to IAM Identity Center.
- Users can use the existing passwords in Microsoft Azure AD or Okta to log in to the user portal and access resources under the associated accounts. The administrator does not need to re-assign passwords.
- Multi-factor authentication
 - The IAM Identity Center administrator can forcibly enable multi-factor authentication (MFA) for users to reduce the risk of password leakage.
 - MFA devices support apps that comply with the Time-Based One-Time Passwords (TOTP) protocol.

Fine-grained Authorization: Assigning Different Permissions on Member Accounts to Different Identities Easily

Figure 2-2 Fine-grained authorization



Generally, a large enterprise has multiple Huawei Cloud accounts, which carry different services and are used by different workforce identities. Different workforce identities need to be configured with fine-grained permissions for access to different member accounts to ensure secure resource access within the enterprise. In this scenario, IAM Identity Center has the following advantages:

- Centralized management of multi-account permissions
 - The IAM Identity Center administrator can create permission sets, each of which contains a maximum of 20 IAM policies.
 - Each account can be associated with permission sets and IAM Identity Center users who are allowed to access resources under the account.

- IAM Identity Center automatically synchronizes the account permission information to IAM without the complexity of managing individual accounts.
- Attribute-based access control
 - The IAM Identity Center administrator can create permission sets based on identity attributes, request context attributes, and resource attributes supported by IAM. These include more than 20 global attributes, such as organizations, tags, request time, and source addresses of users and resources, and other cloud service-level attributes.
 - The IAM Identity Center administrator can create permission sets based on service tags defined by identity providers. IAM Identity Center automatically converts the service tags to the identity tag attributes in IAM during federated login to control access permissions.
 - The administrator configures permissions for all users only once. Permissions can be automatically changed or revoked when the administrator modifies identity tag attributes at later time.

3 Functions

Centralized Identity Management

IAM Identity Center allows you to create and manage users and groups as identities. With login credentials, your users can then manage their own access to multiple Huawei Cloud accounts from a single user portal.

Fine-grained Permissions Management

The IAM Identity Center administrator can configure different identities with permissions specific to each level of your organization for access to different member accounts. These assigned permissions can be changed or revoked at any time.

Integration with Identity Management Systems

IAM Identity Center allows you to grant your workforce users SSO access to SAML 2.0-based identity management systems instead of needing to create new users. This streamlines workforce management while minimizing security risks.

4 Permissions

If you need to assign different permissions to workforce identities in your enterprise to access IAM Identity Center resources on Huawei Cloud, 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 securely access Huawei Cloud resources.

With IAM, you can create IAM users and assign permissions to control their access to specific resources.

You can skip this section if you do not need fine-grained permissions management.

IAM is a free service. You only pay for the resources in your account.

For more information about IAM, see [IAM Service Overview](#).

IAM Identity Center Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

IAM Identity Center is a global service deployed for all regions. When you set the authorization scope to **Global services**, users have permission to access IAM Identity Center in all regions.

You can grant permissions by using roles and policies.

- **Roles:** A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Huawei Cloud services depend on each other. When you grant permissions using roles, you may need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.
- **Policies:** A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only permission to manage

ECSs of a certain type. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions.

Table 1 lists all the system-defined permissions for IAM Identity Center.

Table 4-1 System-defined permissions for IAM Identity Center

Policy Name	Description	Type	Dependency
IAM IdentityCenter FullAccess	Administrator permissions for IAM Identity Center. Users with these permissions can perform all operations on IAM Identity Center.	System-defined policy	None
IAM IdentityCenter ReadOnlyAccess	Read-only permissions for viewing data on IAM Identity Center.	System-defined policy	None

Table 2 lists the common operations supported by system-defined permissions for IAM Identity Center.

Table 4-2 Common operations supported by system-defined permissions

Operation	IAM IdentityCenter FullAccess	IAM IdentityCenter ReadOnlyAccess
Creating a user	√	x
Viewing details about a user	√	√
Modifying user information	√	x
Creating a group	√	x
Adding a user to or removing a user from a group	√	x
Deleting a group	√	x
Viewing details about a group	√	√
Creating a permission set	√	x
Modifying a permission set	√	x
Deleting a permission set	√	x
Viewing details about a permission set	√	√

Helpful Links

- [IAM Service Overview](#)
- [Creating an IAM User and Granting Permission to Use IAM Identity Center](#)

5 Notes and Constraints

Notes

- IAM Identity Center obtains member account information from organizations defined in the Organizations service. Before using IAM Identity Center, you must enable the Organizations service and create an organization. Then, you can log in to IAM Identity Center using the organization's management account. For details about how to enable the Organizations service and create an organization, see [Creating an Organization](#).
- IAM Identity Center of the Huawei Cloud Chinese Mainland website cannot be used to manage accounts on the Huawei Cloud International website, and IAM Identity Center of the Huawei Cloud International website cannot be used to manage accounts on the Huawei Cloud Chinese Mainland website.

Constraints

The following table describes quotas for IAM Identity Center. To increase the quota, see [Quota Adjustment](#).

Table 5-1 Quotas for IAM Identity Center

Item	Default Quota	Adjustable
Number of users that can be created in IAM Identity Center	100,000	Yes
Number of groups that can be created in IAM Identity Center	100,000	Yes
Number of users in a group	Unlimited	-
Number of groups to which a user can be added	1,000	No
Number of virtual multi-factor authentication (MFA) devices that can be added to a user	2	No

Item	Default Quota	Adjustable
Number of permission sets that can be created in IAM Identity Center	2,000	Yes
Number of policies in a permission set	20 system-defined policies and 1 custom policy	No
Number of permission sets that can be associated with a Huawei Cloud account	50	Yes
Number of characters in a custom policy	6,144	No
Number of external identity providers (IdPs) that can be connected	1	No

6 Billing

IAM Identity Center is a free service. You only need to pay for the cloud services and resources used in your accounts. For details about the billing for using resources, see the billing description for each resource.

7 Concepts

IAM Identity Center User

A user created in IAM Identity Center. You can associate an IAM Identity Center user with multiple accounts in your organization and configure permissions for the user. Then, you can log in to the system as the IAM Identity Center user to access resources of those accounts without repeated login.

IAM Identity Center Group

A logical combination of IAM Identity Center users. You can authorize users by adding them to or removing them from groups, facilitating unified permission management. Users added to a group automatically obtain the permissions granted to the group. If a user is added to multiple groups, the user inherits the permissions from all these groups.

Permission Set

A permission template created and maintained by an administrator. It defines one or more IAM policies. Permission sets simplify the assignment of Huawei Cloud account access for users and groups in IAM Identity Center. With permission sets, you do not need to configure permissions for accounts individually.

8 Change History

Released On	Description
2023-08-30	This issue is the first official release.