Enterprise Self-Service Management 25.3.0

Introduction

Issue   06
Date   2025-03-30

Contents

1 What Is ESM?

Enterprise Self-Service Management (ESM) allows you to manage operations of your Huawei dedicated cloud sites on your own. It also offers a broad set of dashboards you can use to gain comprehensive, multi-dimensional data insights into the status and health of your dedicated cloud sites.

Architecture

Figure 1-1 Architecture
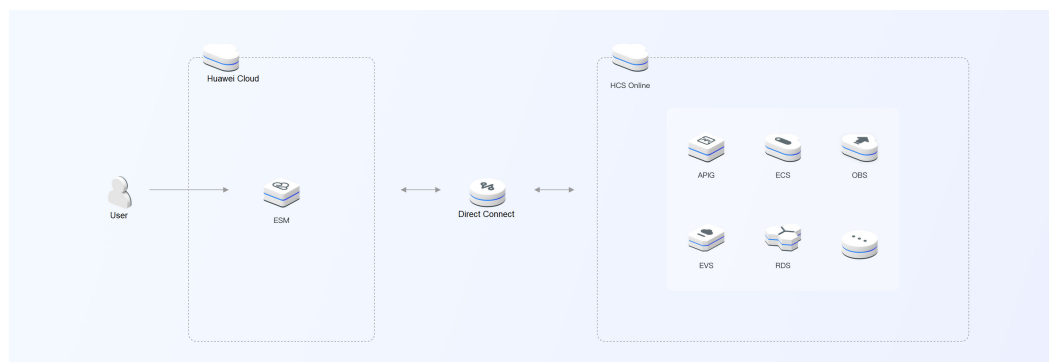
How to Access ESM

You can access ESM from a web console.

You can use a Huawei account that passes real-name authentication to log in to the management console. Then, select or search for **ESM**. If you have not created a Huawei account, perform operations in **Signing Up for a HUAWEI ID and Enabling Huawei Cloud ServicesSigning up for a HUAWEI ID and Enabling Huawei Cloud Services** and **Real-Name Authentication**.

2 Advantages

- Multi-dimensional details

  Dashboards deliver O&M data analysis and display real-time threats on cloud resources. They alert you immediately of any risks and provide deep insights into the resource status.

- Easy to manage

  You can connect ESM to Cloud Trace Service (CTS) for bill management, approval, and audit as well as account management. A customer's cloud management team can independently manage cloud resource usage.

- Continually optimized for better experience

  Version update notifications let you know what's new. ESM can be automatically upgraded and allows for more secure policy-based access control.

3 Scenarios

ESM is used in:

- Internal management: Group companies provide local account management, quota management, and SDR APIs for internal operations of their subsidiaries and branches.

- ToB operations: A complete operations platform and portal are provided for industry cloud and government cloud projects in HCS Online.

Core value: A broad set of dashboards give you deep insights into your resource pools. Anyone authorized to access the dashboards can share data using open APIs. You can register or deregister tenants and configure cloud service quotas to effectively manage resources.

4 Functions

Platform Management

You can create or deregister tenants and manage the cloud platform on your own.

Operations Management

ESM allows you to manage cloud service quotas and metering SDRs so that you can keep abreast of the platform status and effectively manage platform resources.

Data Visualization

Dashboards track and visualize data of resources, tenants, services, applications, and alarms. The data can be shared through open standard APIs. The dashboards can also be connected to a third-party management platform. These capabilities drive digital operations.

5 Security

5.1 Data Protection Technologies

To prevent personal data (such as the username or password) from being accessed by unauthorized entities or individuals, ESM takes different measures to keep data secure and reliable.

Collecting Personal Data

Table 5-1 describes the personal data generated or collected by ESM.

Table 5-1 List of personal data

Type	Collection Method	Purpose	Modifiable	Mandatory	Lifecycle Management
User Name	You register a Huawei Cloud account.	Notify you of the ticket processing progress.	Yes	Yes	Deleted when you delete your account
IP	You use the service.	Record audit logs.	No	Yes	Deleted when logs are cleared

Type	Collection Method	Purpose	Modifiable	Mandatory	Lifecycle Management
Ticket information	You submit tickets and leave messages. The information includes the problem descriptions, left messages, and uploaded log screenshots.	● Create tickets and leave messages and information requested by Huawei Cloud engineers during the ticket processing to quickly and accurately locate and handle your problems. ● Do not include sensitive personal data, such as passwords and mobile numbers, in problem descriptions, left messages, and log files.	No	Yes	Ticket information is necessary for ticket processing and will be stored for quality inspection and audit purposes for a long time.

Type	Collection Method	Purpose	Modifiable	Mandatory	Lifecycle Management
Email address	• You submit a ticket. • You register a Huawei Cloud account.	• The email addresses you provided during ticket submission are used to notify you of the ticket processing progress. • The registered email address is used only as the emergency contact information. During ticket processing and return visits, Huawei Cloud will preferentially contact you using the email addresses you provided during the ticket submission.	Yes	No	• Any email address newly authenticated on the ticket submission page will be deleted after the validity period (three months) expires. • The involved tickets are processed. • You can submit a request to ask for deleting the mobile numbers and email addresses you provided during the ticket submission. • The registered email address and mobile number will be deleted when you delete your Huawei Cloud account.

Type	Collection Method	Purpose	Modifiable	Mandatory	Lifecycle Management
Mobile number	- You submit a ticket. - You register a Huawei Cloud account.	- The mobile numbers you provided during ticket submission are used to notify you of the ticket processing progress. - The registered mobile number is used only as the emergency contact information. During ticket processing and return visits, Huawei Cloud will preferentially contact you using the mobile numbers you provided during the ticket submission.	Yes	No	

Storage Mode

The ticket system uses encryption algorithms to encrypt the following sensitive data and then stores the encrypted data:

- The following personal sensitive data is encrypted before storage: Email addresses, mobile numbers, and authorized information.

- Ticket information is not personal sensitive data and therefore is stored in plaintext.

Access Permissions

Only whitelisted personnel are allowed to access your encrypted data stored in the ticket database.

API Constraints

IAM token-based authentication is required for calling APIs.

6 Permission Management

ESM Permissions

New IAM users do not come with default permissions, so add them to one or more groups and then attach policies or roles to these groups to grant specific operation permissions on cloud services.

You can grant permissions to a role or by creating a policy.

- Roles: A coarse-grained IAM authorization strategy to assign permissions based on user responsibilities. IAM provides a limited number of roles for permission management. When grant permissions to a role, you also need to assign other roles on which the permissions depend. Roles are not an ideal choice for fine-grained authorization and secure access control.

- Policies: A fine-grained authorization tool that defines permissions for operations on specific cloud resources under certain conditions. This mechanism enables more flexible authorization and meets secure access control requirements. Most policies define permissions based on APIs. For API actions supported by ESM, see ESM policies and supported actions.

Table 6-1 lists all the system policies supported by ESM.

Table 6-1 ESM system permissions

Policy	Description	Type	Suggestion
ESM FullAccess	Administrator permission on all ESM functions	System policy	Assign this policy to administrators who create or deregister tenants.
ESM ReadOnly Access	Read-only permission on ESM	System policy	Assign this policy to administrators who use dashboards.

Supported Actions

Actions supported by a system policy vary depending on APIs in use.

- Permissions: statements in a policy that allow or deny certain operations
- Actions: actions supported by system policies

Table 6-2 Supported actions

Policy	Permission	Action
ESM FullAccess	HCS Online site management	esm:hcso:get esm:hcso:list esm:hcso:update
	HCS Online tenant management	esm:hcsoTenant:create esm:hcsoTenant:delete esm:hcsoTenant:get esm:hcsoTenant:list esm:hcsoTenant:update esm:hcsoTenantOwnerUser:create esm:hcsoTenantOwnerUser:update
	HCS Online project query	esm:hcsoProject:list
	Quota management	esm:hcsoQuota:get esm:hcsoQuota:update
	Visualization	esm:hcsoDashboard:use
	Alarm notification management	esm:hcsoDashboard:create esm:hcsoDashboard:get esm:hcsoDashboard:delete esm:hcsoDashboard:update esm:hcsoDashboard:list
	Logo update	esm:DashboardLogo:put
ESM ReadOnlyAccess	Read-only for HCS Online sites	esm:hcso:get esm:hcso:list
	Read-only for HCS Online tenants	esm:hcsoTenant:get esm:hcsoTenant:list
	HCS Online project query	esm:hcsoProject:list
	Read-only quota	esm:hcsoQuota:get
	Visualization	esm:hcsoDashboard:use
	Read-only alarm notification	esm:hcsoDashboard:get esm:hcsoDashboard:list

7 Constraints

ESM has been put into commercial use. However, network security dashboards are unavailable.

8 Change History

Released On	Description
2025-03-30	This issue is the sixth official release.
2024-11-30	This issue is the fifth official release.
2024-07-30	This issue is the fourth official release.
2024-04-30	This issue is the third official release.
2023-11-30	This issue is the second official release.
2023-10-30	This issue is the first official release.