

SecMaster

User Guide

Issue 02
Date 2023-09-20



Copyright © Huawei Cloud Computing 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 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.

Contents

1 Service Overview	1
1.1 What Is SecMaster?	1
1.2 Features and Functions	1
1.3 Product Advantages	6
1.4 Application Scenarios	6
1.5 Billing	7
1.6 Permissions Management	8
1.7 SecMaster and Other Services	9
1.8 Basic Concepts	10
2 Authorizing SecMaster	12
3 Editions	14
3.1 Buying a Value-Add Pack	14
3.2 Increasing the Quota	15
3.3 Unsubscribing from SecMaster	16
4 Security Overview	17
4.1 Overview	17
4.2 Security Score	21
5 Workspaces	24
5.1 Workspace Overview	24
5.2 Creating a Workspace	24
5.3 Managing Workspaces	26
5.3.1 Viewing Workspace Details	26
5.3.2 Editing a Workspace	28
5.3.3 Deleting a Workspace	28
6 Viewing Purchased Resources	30
7 Security Situation	31
7.1 Situation Overview	31
7.2 Large Screen	38
7.2.1 Overall Situation Screen	38
7.2.2 Monitoring Statistics Screen	40
7.2.3 Asset Security Screen	42

7.2.4 Threat Situation Screen.....	43
7.2.5 Vulnerable Assets Screen.....	45
7.3 Reports.....	46
7.3.1 Creating or Copying a Report.....	46
7.3.2 Viewing a Security Report.....	48
7.3.3 Downloading a Report.....	50
7.3.4 Managing Security Reports.....	51
7.4 Task Center.....	53
7.4.1 Viewing To-Do Tasks.....	53
7.4.2 Handling a To-Do Task.....	54
8 Resource Manager.....	56
8.1 Resource Manager Overview.....	56
8.2 Modifying the Asset Information Synchronization Policy.....	57
8.3 Viewing Resource Information.....	59
8.4 Importing and Exporting Assets.....	63
8.5 Deleting an Asset.....	77
9 Risk Prevention.....	79
9.1 Baseline Inspection.....	79
9.1.1 Cloud Service Baseline Overview.....	79
9.1.2 Configuring a Baseline Inspection Plan.....	79
9.1.3 Executing a Baseline Inspection Plan.....	81
9.1.4 Handling Manual Check Items.....	83
9.1.5 Viewing Baseline Inspection Results.....	84
9.1.6 Handling Baseline Inspection Results.....	86
9.2 Vulnerability Management.....	91
9.2.1 Vulnerability Management Overview.....	91
9.2.2 Viewing Vulnerability Details.....	92
9.2.3 Fixing Vulnerabilities.....	94
9.2.4 Importing and Exporting Vulnerabilities.....	97
9.2.5 Ignoring and Unignoring a Vulnerability.....	110
10 Threat Operations.....	112
10.1 Incident Management.....	112
10.1.1 Viewing an Incident.....	112
10.1.2 Adding or Editing an Incident.....	114
10.1.3 Importing and Exporting Incidents.....	118
10.1.4 Closing or Deleting Incidents.....	124
10.2 Alert Management.....	126
10.2.1 Viewing Alerts.....	126
10.2.2 Converting an Alert to an Incident.....	128
10.2.3 Adding or Editing an Alert.....	129
10.2.4 Importing and Exporting Alerts.....	133

10.2.5 Closing or Deleting an Alert.....	139
10.3 Indicator Management.....	141
10.3.1 Creating an Indicator.....	141
10.3.2 Disabling Indicators.....	143
10.3.3 Importing and Exporting Intelligence Indicators.....	144
10.3.4 Managing Indicators.....	149
10.4 Intelligent Modeling.....	153
10.4.1 Viewing Existing Model Templates.....	153
10.4.2 Creating/Editing a Model.....	154
10.4.3 Viewing Existing Models.....	164
10.4.4 Managing Models.....	165
10.5 Security Analysis.....	166
10.5.1 Security Analysis Overview.....	166
10.5.2 Getting Started.....	166
10.5.3 Configuring Indexes.....	167
10.5.4 Querying and Analyzing Data.....	169
10.5.5 Downloading Logs.....	174
10.5.6 Query and Analysis Syntax.....	175
10.5.6.1 SQL Syntax.....	175
10.5.6.1.1 Basic Syntax.....	175
10.5.6.1.2 Query Statements.....	175
10.5.6.1.3 Analysis Statements.....	177
10.5.6.1.4 Limitations and Constraints.....	188
10.5.6.2 Quick Query.....	188
10.5.7 Quickly Adding a Log Alarm Model.....	190
10.5.8 Charts.....	194
10.5.8.1 Overview.....	194
10.5.8.2 Tables.....	194
10.5.8.3 Line Charts.....	196
10.5.8.4 Bar Charts.....	198
10.5.8.5 Pie Charts.....	201
10.5.9 Managing Data Spaces.....	203
10.5.9.1 Creating a Data Space.....	203
10.5.9.2 Viewing Data Space Details.....	204
10.5.9.3 Editing a Data Space.....	206
10.5.9.4 Deleting a Data Space.....	207
10.5.10 Managing Pipelines.....	208
10.5.10.1 Creating a Pipeline.....	208
10.5.10.2 Viewing Pipeline Details.....	210
10.5.10.3 Editing a Pipeline.....	212
10.5.10.4 Deleting a Pipeline.....	213
10.6 Data Consumption.....	215

10.7 Data Delivery.....	216
10.7.1 Creating a Data Delivery.....	216
10.7.2 Data Delivery Authorization.....	220
10.7.3 Checking the Data Delivery Status.....	222
10.7.4 Managing Data Delivery.....	224
10.8 Data Monitoring.....	227
11 Security Orchestration.....	230
11.1 Security Orchestration Overview.....	230
11.2 Security Orchestration Process.....	231
11.3 Configuring and Enabling a Workflow.....	231
11.4 Configuring and Enabling a Playbook.....	236
11.5 Operation Object Management.....	238
11.5.1 Data Class.....	238
11.5.1.1 Viewing Data Classes.....	238
11.5.2 Type Management.....	239
11.5.2.1 Managing Alert Types.....	239
11.5.2.2 Managing Incident Types.....	246
11.5.2.3 Managing Threat Intelligence Types.....	252
11.5.2.4 Managing Vulnerability Types.....	259
11.5.3 Classification & Mapping.....	265
11.5.3.1 Creating a Classification and Mapping.....	266
11.5.3.2 Managing Category Mappings.....	267
11.6 Playbook Orchestration Management.....	272
11.6.1 Playbooks.....	272
11.6.1.1 Submitting a Playbook Version.....	272
11.6.1.2 Reviewing a Playbook Version.....	273
11.6.1.3 Enabling a Playbook.....	274
11.6.1.4 Managing Playbooks.....	275
11.6.1.5 Managing Playbook Versions.....	280
11.6.2 Workflows.....	284
11.6.2.1 Reviewing a Workflow Version.....	284
11.6.2.2 Enabling a Workflow.....	286
11.6.2.3 Managing Workflows.....	287
11.6.2.4 Managing Workflow Versions.....	291
11.6.3 Asset Connections.....	297
11.6.3.1 Adding an Asset Connection.....	297
11.6.3.2 Managing Asset Connections.....	298
11.6.4 Instance Management.....	302
11.6.4.1 Viewing Monitored Playbook Instances.....	302
11.7 Layout Management.....	304
11.7.1 Viewing an Existing Layout Template.....	304
11.7.2 Manage Existing Layouts.....	305

11.8 Plug-in Management.....	306
11.8.1 Overview.....	306
11.8.2 Viewing Plug-in Details.....	307
12 Settings.....	308
12.1 Data Collection.....	308
12.1.1 Data Collection Overview.....	308
12.1.2 Buying an ECS.....	310
12.1.3 Installing the Agent.....	312
12.1.4 Creating a Node.....	315
12.1.5 Configuring a Component.....	316
12.1.6 Adding a Connection.....	317
12.1.7 Configuring a Parser.....	318
12.1.8 Adding a Collection Channel.....	320
12.1.9 Collection Management.....	323
12.1.9.1 Managing Connections.....	323
12.1.9.2 Managing Parsers.....	325
12.1.9.3 Managing Collection Channels.....	328
12.1.9.4 Managing Collection Nodes.....	333
12.1.10 Component Management.....	334
12.1.10.1 Managing Collection Nodes.....	334
12.1.10.2 Managing Components.....	337
12.2 Data Integration.....	338
12.2.1 Access Data.....	338
12.3 Checks.....	341
12.4 Customizing Directories.....	342
13 Permissions Management.....	345
13.1 Creating a User and Granting Permissions.....	345
13.2 SecMaster Custom Policies.....	347
13.3 SecMaster Permissions and Supported Actions.....	348
14 FAQs.....	349
14.1 Product Consulting.....	349
14.1.1 What Is SecMaster?.....	349
14.1.2 Why Is There No Attack Data or Only A Small Amount of Attack Data?.....	349
14.1.3 What Are Data Sources of SecMaster?.....	349
14.1.4 What Are the Dependencies and Differences Between SecMaster and Other Security Services?...	350
14.1.5 What Are the Differences Between SecMaster and HSS?.....	351
14.1.6 How Do I Update My Security Score?.....	353
14.1.7 How Do I Handle a Brute-force Attack?.....	353
14.1.8 Why Is the Incident Data in SecMaster Inconsistent with That in WAF and HSS?.....	355
14.1.9 Troubleshooting the Agent Installation Failure.....	355
14.1.10 How Do I Grant Permissions to an IAM User?.....	359

14.2 Purchase Consulting.....	360
14.2.1 How Do I Change SecMaster Editions or Specifications?.....	360
14.2.2 How Is SecMaster Billed?.....	360
14.2.3 Can I Unsubscribe from SecMaster?.....	360
A Change History.....	362

1 Service Overview

1.1 What Is SecMaster?

SecMaster is a next-generation cloud native security operation platform. It enables integrated and automatic security operations through cloud asset management, security posture management, security information and incident management, security orchestration and automatic response, cloud security overview, simplified cloud security configuration, configurable defense policies, and intelligent and fast threat detection and response.

1.2 Features and Functions

Based on cloud native security, SecMaster provides a comprehensive closed-loop security handling process that contains log collection, security governance, intelligent analysis, situation awareness, and orchestration response, helping you protect cloud security.

SecMaster provides [Security Overview](#), [Workspace Management](#), [Security Situation](#), [Asset Management](#), [Risk Prevention](#), [Security Response](#), [Security Orchestration](#), [Data Collection](#), and [Data Integration](#).

Security Overview

It displays a comprehensive overview of asset security situation together with other linked cloud security services.

Table 1-1 Functions

Function Module	Description
Security Score	SecMaster evaluates and scores your cloud asset security. You can quickly learn of unhandled risks and their threats to your assets. The lower the security score, the greater the overall asset security risk.

Function Module	Description
Security Monitoring	You can view how many threats, vulnerabilities, and compliance risks that are not handled and view details of them.
Your Security Score over Time	You can view your security scores for the last 7 days.

Workspace Management

Workspaces are top-level workbenches in SecMaster. A single workspace can be bound to common projects, to support workspace operation modes in different application scenarios.

Table 1-2 Functions

Function Module	Description
Workspaces	A single workspace can be bound to common projects to support workspace operation modes in different scenarios.

Security Situation

You can view the security overview on the large screen in real time and periodically subscribe to security operation reports to know the core security indicators.

Table 1-3 Functions

Function Module	Description	
Situation Overview	Security Score	The lower the security score, the greater the overall asset security risk.
	Security Monitoring	You can view how many threats, vulnerabilities, and compliance risks that are not handled and view details of them.
	Your Security Score over Time	You can view your security scores for the last 7 days.

Function Module	Description
Large Screen	AI analyzes and classifies massive cloud security data and then displays security incidents in real time on a large screen. The large screen display gives you a simple, intuitive, bird's eye view of the security of your entire network clearly and efficiently.
Reports	You can generate analysis reports. In this way, you can learn about the security status of your assets in a timely manner.
Task Center	Displays the tasks to be processed in a centralized manner.

Asset Management

SecMaster automatically discovers and manages all assets on and off the cloud and displays the real-time security status of your assets.

Table 1-4 Functions

Function Module	Description
Resource Manager	Synchronizes the security statistics of all resources and allows you to view the name, service, and security status of a resource, helping you quickly locate security risks.

Risk Prevention

Risk prevention provides baseline check and vulnerability management functions to help your cloud security configurations meet various authoritative security standards, understand the global vulnerability distribution.

Function Module	Description
Baseline Inspection	SecMaster can scan cloud baseline configurations to find out unsafe settings, report alerts for incidents, and offer hardening suggestions to you.
Vulnerabilities	Automatically synchronizes vulnerability scanning result from Host Security Service (HSS), displays vulnerability scanning details by category, allows users to view vulnerability details, and provides vulnerability fixing suggestions.

Security Response

Threat operation provides various threat detection models to help you detect threats from massive security logs and generate alerts; provides various security response playbooks to help you automatically analyze and handle alerts, and automatically harden security defense and security configurations.

Table 1-5 Functions

Function Module		Description
Incidents		Displays incident details in a centralized manner and supports manually or automatically turning alerts into incidents.
Alerts		Integrates and displays alerts of various cloud services, including HSS, WAF, and Anti-DDoS.
Indicators		Integrates indicators of many cloud services and extracts indicators based on custom alert and incident rules.
Intelligent Modeling		Alert models can be built.
Security Analysis	Query and Analysis	<ul style="list-style-type: none"> • Search and analysis: Supports quick data search and analysis, quick filtering of security data for security survey, and quick locating of key data. • Statistics filtering: SecMaster supports quick analysis and statistics of data fields and quick data filtering based on the analysis result. Time series data supports statistics collection by default time partition, allowing data volume trend to be quickly spotted. SecMaster supports analysis, statistics, and sorting functions, and supports quick building of security analysis models. • Visualization: Visualized data analysis intuitively reflects service structure and trend, enabling customized analysis reports and analysis indicators to be easily created.
	Data Monitoring	Supports end-to-end data traffic monitoring and management.
	Data Consumption	<ul style="list-style-type: none"> • Provides streaming communication interfaces for data consumption and production, provides data pipelines that are integrated with SDKs, and allows customers to set policies for data production and consumption. • Provides Logstash open-source collection plug-ins for data consumption and production.

Security Orchestration

Security Orchestration supports playbook management, process management, data class management (security entity objects), and asset connection management. You can also customize playbooks and processes.

Security Orchestration allows you to flexibly orchestrate security response playbooks through drag-and-drop according to your service requirements. You can also flexibly extend and define security operation objects and interfaces.

Table 1-6 Functions

Function Module	Description
Objects	Manages operation objects such as data classes, data class types, and category mappings in a centralized manner.
Playbooks	Supports full lifecycle management of playbooks, processes, connections, and instances.
Layouts	Provides a visualized low-code development platform for customized layout of security analysis reports, alarm management, incident management, vulnerability management, baseline management, and threat indicator library management.
Plugins	Plug-ins used in the security orchestration process can be managed in a unified manner.

Data Collection

Collects various log data in multiple modes. After data is collected, historical data analysis and comparison, data association analysis, and unknown threat discovery can be quickly implemented.

Table 1-7 Functions

Function Module	Description
Collectors	Logstash is used to collect various log data in multiple modes. After data is collected, historical data analysis and comparison, data association analysis, and unknown threat discovery can be quickly implemented.

Data Integration

Integrate security ecosystem products for associated operations or data interconnection. After the integration, you can search for and analyze all collected logs.

Table 1-8 Functions

Function Module	Description
Data Integration	The built-in log collection system supports one-click integration of logs from cloud products, covering storage, management, monitoring, and security. After the integration, you can search for and analyze all collected logs.

1.3 Product Advantages

Refined Indicators and Intuitive Situation Display

You can view the security overview on the large screen in real time and periodically subscribe to security operation reports to know the core security indicators.

Cloud Native Asset Stocktaking and Risk Prevention

All assets and security configurations on the cloud are automatically checked, and automatic hardening is provided to help you fix risky assets and insecure configurations. This avoids implicit channels and security device vulnerabilities introduced by traditional bolted-on security solutions.

Intelligent and Efficient Threat Detection, Response, and Handling

SecMaster focuses on finding true threats. Based on analysis of trillions of security logs every day, years of experience, and built-in machine learning (AI models and analysis playbooks), SecMaster can sift out normal incidents. Threat and asset security profiling enables restoration of the entire attack chain. Risk handling playbooks can be configured for automatic response, simplifying operations and improving security and efficiency.

Environment Integration and Operational Collaboration for Ultimate Flexibility

You can connect to all security products, devices, and tools to connect data and operations (Bidirectional interconnection is supported). You can also define your own response models and analysis/handling playbooks to best meet your security requirements. You can use workspaces to enable large-scale organization collaboration and MSSP (Managed Security Service Provider) services.

1.4 Application Scenarios

The principle of cloud security is "30% R&D + 70% Operations". The "70% Operations" is where SecMaster is applied. The specific application scenarios of SecMaster are as follows:

Routine Security Operation

Inspect check items and implement the security operation process to achieve security objectives. Identify and mitigate risks, and continuously improve the process to prevent risk recurrence.

Key Incident Assurance

Provide 24/7 assurance during major festivals, holidays, activities, and conferences through attack defense to ensure service availability.

Security Drills

Provides security assurance in the attack defense drills organized by regulatory institutions through intrusion prevention, helping organizations pass the assessments in the drills.

Security Evaluation

Perform the white box baseline test, black box attack surface assessment, and attack vector detection before key incidents or drills to identify vulnerabilities.

1.5 Billing

Billing Items

SecMaster's **professional edition** is billed based on the purchased asset quota and optional value-added packs.

Table 1-9 Billing items

Edition	Billing Item	Description
Professional	Asset quota	Billed based on purchased asset quota, including the total ECS quota and website quota.
	Pay-per-use billing	Enabled or disabled at any time and billed for usage by the hour.
Value-added pack	Large screen	Billed based on usage duration. Enabled at additional cost. There is an additional fee for the Large Screen.
	Intelligent analysis quota	Billed based on the actual traffic usage. Enabled at additional cost. If intelligent search and analysis are required, you need to pay extra fees in addition to your purchased asset quota.
	Security orchestration	Billed based on the actual number of use times. Enabled at additional cost. You need to additionally pay for this function.

Billing Modes

SecMaster is billed in pay-per-use mode. In this mode, you are billed for usage duration by the hour. This mode allows you to enable or disable the SecMaster service at any time.

Changing Billing Options

- Changing asset quotas
If the number of your assets increases, you can increase the asset quotas in the same billing mode. A scale-down of purchased quotas is not supported.
- Enabling the **Plus Packs**
You can pay an extra fee to have the plus features, such as **Large Screen**, **Intelligent Analysis**, and **Security Orchestration**.

NOTICE

The **Large Screen**, **Intelligent Analysis**, and **Security Orchestration** in the value-added packages are plus features of the professional edition. To use them, purchase the professional edition first.

1.6 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your SecMaster resources, 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.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, you can use policies to grant different permissions to software developers in your enterprises to allow them to only use SecMaster but not perform certain high-risk operations, such as deletion of SecMaster data.

If your account does not need individual IAM users for permissions management, then you may skip over this chapter.

IAM is free. You pay only for the resources in your account. For more information about IAM, see [IAM Service Overview](#).

SecMaster Permissions

By default, new IAM users do not have any permissions assigned. You can add a user to one or more groups to allow them to inherit the permissions from the groups to which they are added.

SecMaster is a project-level service deployed and accessed in specific physical regions. To assign permissions to a user group, specify the scope as region-specific

projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. To access SecMaster, the users need to switch to a region where they have been authorized to use cloud services.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. Only a limited number of service-level roles for authorization are available. You need to also assign other dependent roles for the permission control to take effect. Roles are not ideal 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 meets secure access control requirements. For example, you can grant SecMaster users only the permissions for managing a certain type of resources.

Table 1-10 lists all SecMaster system permissions.

Table 1-10 System-defined permissions supported by SecMaster

Policy Name	Description	Type	Dependency
SecMaster FullAccess	All permissions of SecMaster.	System-defined policy	None
SecMaster ReadOnlyAccess	SecMaster read-only permission. Users granted with these permissions can only view SecMaster data but cannot configure SecMaster.	System-defined policy	None

1.7 SecMaster and Other Services

This topic describes SecMaster and its linked services.

Security Services

SecMaster obtains necessary security incident records from security services such as Host Security Service (HSS) and Web Application Firewall (WAF). SecMaster then uses big data mining and machine learning to intelligently analyze and identify attacks and intrusions, helping you understand the attack and intrusion processes. SecMaster also provides helpful protective measures for you.

Elastic Cloud Server (ECS)

SecMaster detects threats to your ECSs with linked service HSS, comprehensively displays ECS security risks, and provides protection suggestions.

1.8 Basic Concepts

This topic describes concepts used in SecMaster.

Security Risk

A security risk is a comprehensive evaluation of your assets, reflecting the security level of your assets within a period of time by a security score. A security score is for your reference to know the security situation of your assets.

Threat Alert

In general, threat alerts refer to threats that, due to natural, human, software, or hardware reasons, are detrimental to information systems or cause negative effects on the society. In SecMaster, threat alerts are detected security incidents that threaten asset security through big data technology.

Workspace

Workspaces are the root of SecMaster resources. A single workspace can be bound to general projects, enterprise projects, and regions for different application scenarios.

Data Space

A data space is a unit for data grouping, load balancing, and flow control. Data in the same data space shares the same load balancing policy.

Data Pipelines

A data transfer message topic and a storage index form a pipeline.

Classification and Mapping

Type matching and field mapping for cloud service alarms.

Security Orchestration

Security orchestration is a process that combines security capabilities (applications) and manual checks based on certain logical relationships to complete a specific security operations procedure. Security functions of different security operations systems or components are encapsulated through programmable interfaces (APIs) during this process.

Security orchestration is a collaborative work mode that integrates various capabilities related to security operations, such as tools/technologies, workflows, and personnel.

Producer

A producer is a logical object used to construct data and transmit it to the server. It stores data in message queues.

Subscriber

A subscriber is used to subscribe to SecMaster pipeline messages. A pipeline can be subscribed to by multiple subscribers. SecMaster distributes messages through subscribers.

Consumer

A consumer is a running entity that receives and processes data. It consumes and processes messages in the SecMaster pipeline through subscribers.

Message Queue

A message queue is the container for data storage and transmission.

Threat Detection Model

A threat detection model is a trained AI recognition algorithm model. A threat detection model can automatically aggregate, analyze, and generate alerts for specific threats. This type of model has good generalization and anti-evasion capabilities. They can work in different service systems to defend against sophisticated emerging attacks.

2 Authorizing SecMaster


Before using SecMaster, you need to authorize SecMaster to access some services. If you have obtained such permissions, skip over this section.

Prerequisites

- The IAM account has been authorized. For details, see [How Do I Grant Permissions to an IAM User?](#)
- You have purchased SecMaster.

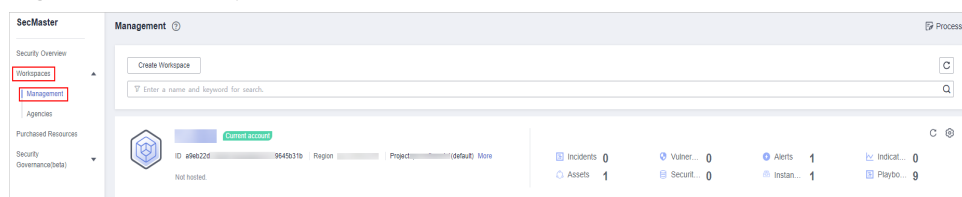
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

Step 3 In the navigation pane, choose **Workspaces > Management**.

Figure 2-1 Workspaces



Step 4 In the upper part of the workspace management page, choose **Entrusted Service Authorization - Current Tenant**.

Figure 2-2 Authorizing for SecMaster



Step 5 On the page for assigning permissions, select all required permissions (which are selected by default), select **Agree to authorize**, and click **Confirm**.

----End

3 Editions

3.1 Buying a Value-Add Pack

In addition to the professional edition, SecMaster also provides value-added features for you to choose.

Limitations and Constraints

- The value-added package is an additional payment item for the professional edition. To use the value-added package, you need to purchase the professional edition first.

Purchasing a Pay-per-Use Value-added Package

Step 1 In the navigation pane on the left, choose **Purchased Resources**. On the page that is displayed, click **Buy Value-added Package** in the upper right corner. The **Buy Value-added Package** page is displayed.

Step 2 On the **Buy Value-added Package** page, configure required parameters.

1. Select a billing mode, region, and project.
 - **Billing mode:** Select **Pay-per-use**.
 - **Region:** Select a region.
2. **Configuration:** configuration information of the purchased SecMaster version
3. Select functions based on your requirements.

Figure 3-1 Purchasing a value-added package

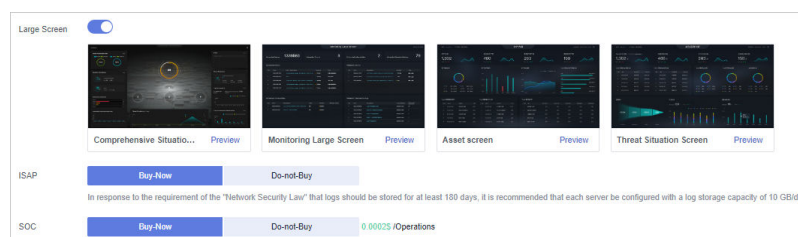




Table 3-1 Purchasing a value-added package

Feature	Buy Now	Do Not Buy
Large Screen	Toggle on the  button next to Large Screen to buy the large screen function.	Retain the toggle-off status ().
ISAP	Select Buy-Now next to ISAP .	Select Do-not-Buy .
SOC	Select Buy-Now after to SOC .	Select Do-not-Buy .

Step 3 Confirm the product details and click **Next**.

Step 4 After confirming that the order details are correct, read the *SecMaster Disclaimer*, select **I have read and agree to the SecMaster Disclaimer**, and click **Pay Now**.

Step 5 On the payment page, select a payment method and complete the payment.

----End

3.2 Increasing the Quota

SecMaster allows you to increase **ECS Quota** and change required duration at any time after you make a purchase.

Limitations and Constraints

- The ECS quota is the total number of ECSs that are authorized to receive checks. The maximum ECS quota cannot exceed 10,000.
- When buying SecMaster, ensure that the total ECS quota is greater than or equal to the total number of ECSs under the current account. Otherwise, threats may not be detected in a timely manner if unauthorized hosts are attacked, adding more risks such as data leakage.

Pay-Per-Use Billing Mode

Step 1 In the navigation pane on the left, choose **Purchased Resources**. Then, click **Increase Quota**.

Step 2 On the page for buying SecMaster, view the current configuration and specify **ECS Quota**.

Note that you only need to increase quotas for ECSs you expect to add.

Step 3 Click **Pay Now**.

Step 4 Return to the SecMaster console. You can start to protect the newly added hosts based on the increased quota.

----End

3.3 Unsubscribing from SecMaster

If you no longer need SecMaster, unsubscribe from it or cancel it with just a few clicks.

- Pay-per-use billing mode: pay for what you use by the hour. This mode allows you to enable or disable resources at any time. One-click resource cancellation is also supported.

Limitations and Constraints

- In the **pay-per-use** professional edition, when you unsubscribe from or cancel the asset quota of the professional edition, the plus package is also unsubscribed or canceled.

Canceling Pay-per-Use SecMaster Resources

Step 1 Click **Professional** in the upper right corner. The edition management window is displayed.

Step 2 In the row of the SecMaster edition purchased in pay-per-use billing mode, click **Cancel** to release the purchased SecMaster resources.

Go to the edition management window and verify that the subscription to resources billed on a pay-per-use basis is canceled.

----End

Unsubscribing from a Plus Features

Step 1 Click **Professional** in the upper right corner. A window for you to manage SecMaster assets will be displayed.

Step 2 Click **Cancel** to release the pay-per-use asset quota. Go to the edition management window and verify that the pay-per-use asset quota is canceled.

----End


4 Security Overview

4.1 Overview

The **Security Overview** page gives you a comprehensive overview of your asset security posture in real time together with other linked cloud security services to collectively display security assessment findings. On the **Security Overview** page, you can view security status of your cloud resources, take required actions with just a few clicks, and manage risks centrally.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

Step 3 In the navigation pane on the left, choose **Security Overview**.

Step 4 On the **Security Overview** page, you can view the security overview of your assets and perform related operations. The **Security Overview** page consists of the following modules:

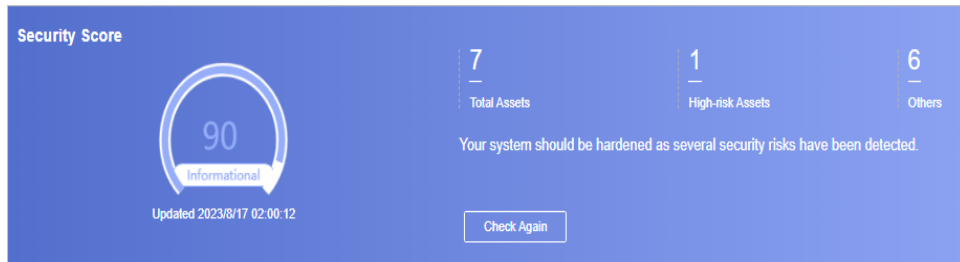
- [Security Score](#)
- [Security Monitoring](#)
- [Your Security Score over Time](#)

----End

Security Score

The security score shows the overall health status of your workloads on the cloud so you can quickly learn of unhandled risks and their threats to your assets.

Figure 4-1 Security Score



- The score ranges from 0 to 100. The higher the security score, the more secure your assets. For details, see [Security Score](#).
- Different color blocks in the security score ring chart indicate different severity levels. For example, yellow indicates that your security is medium.
- The security score is updated when you refresh status of the alert incident after risk handling. After you fix the risks, you can click **Check Again** so that SecMaster can check and score your system again.

NOTE

After risks are fixed, manually ignore or handle alert incidents and update the alert incident status in the alert list. The risk severity can be down to a proper level accordingly.

- The security score reflects the security situation of your system last time you let SecMaster check the system. To obtain the latest score, click **Check Again**.

Security Monitoring

The **Security Monitoring** area includes **Threat Alarms**, **Vulnerabilities**, and **Abnormal Baseline Settings**, which sort risks that have not been handled.

Figure 4-2 Security Monitoring

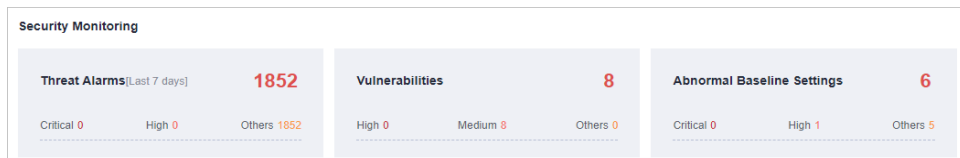


Table 4-1 Security Monitoring parameters

Parameter	Description
Threat Alarms	<p>This panel displays the unhandled threat alerts for the last 7 days. You can quickly learn of the total number of unhandled threat alerts and the number of vulnerabilities at each severity level.</p> <ul style="list-style-type: none"> • Risk severity levels: <ul style="list-style-type: none"> - Critical: There are intrusions to your workloads, and you should view alert details and handle the alert in a timely manner. - High: There are abnormal incidents on your workloads, and you should view alert details and handle the alert in a timely manner. - Others: There are risky incidents that are marked as medium-risk, low-risk, and informational alerts detected in your systems, and you should view alert details and take necessary actions. • To quickly view details of top 5 threat alerts for the last 7 days, click the Threat Alarms panel. <ul style="list-style-type: none"> - You can view details of those threats, including the threat alert name, severity, asset name, and discovery time. - If no data is available here, no threat alerts are generated for the last 7 days.

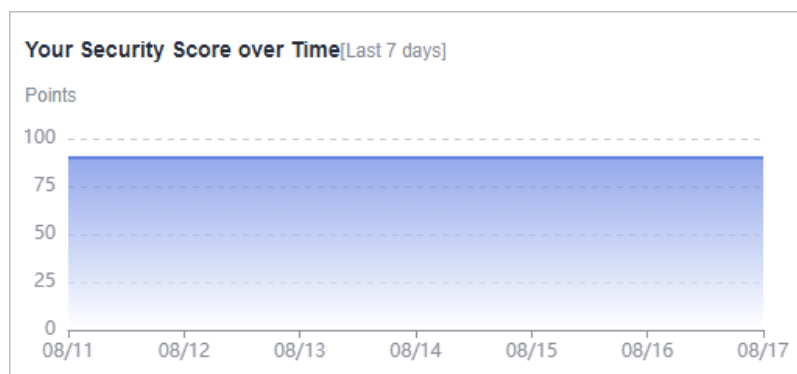
Parameter	Description
Vulnerabilities	<p>This panel displays the top five vulnerability types and the total number of unfixed vulnerabilities in your assets for the last 7 days. You can quickly learn of the total number of unfixed vulnerabilities and the number of vulnerabilities at each severity level.</p> <ul style="list-style-type: none"> ● Risk severity levels: <ul style="list-style-type: none"> – High: There are vulnerabilities on your workloads, and you should view vulnerability details and handle them in a timely manner. – Medium: There are abnormal incidents on your workloads, and you should view vulnerability details and handle the vulnerability in a timely manner. – Others: There are risky incidents that are marked as low-risk or informational in your systems, and you should view vulnerability details and take necessary actions. ● When you click the Top 5 Vulnerability Types tab, the system displays top 5 vulnerability types. <ul style="list-style-type: none"> – Vulnerability rankings are based on the number of hosts a vulnerability affects. The vulnerability ranked the first affects the most hosts. – The data is displayed in Top 5 Vulnerability Types only when the hosts have Host Security Service (HSS) Agent version 2.0 installed. If no data is displayed or you want to view top 5 vulnerability types, upgrade Agent from 1.0 to 2.0. ● Click Top 5 Real-Time Vulnerabilities tab. The system displays the top 5 vulnerability incidents for the last 7 days. You can quickly view vulnerability details. <ul style="list-style-type: none"> – You can view details such as the vulnerability name, severity, asset name, and discovery time. – If no data is available here, no vulnerabilities are detected on the current day.

Parameter	Description
Abnormal Baseline Settings	<p>This panel displays the total number of abnormal baseline settings detected for the last 30 days. You can quickly learn of how many risks are discovered by severity level.</p> <ul style="list-style-type: none"> • Risk severity levels: <ul style="list-style-type: none"> - Critical: There are intrusions to your workloads, and you should view details about abnormal baseline settings and handle them in a timely manner. - High: There are abnormal incidents on your workloads, and you should view details about compliance risks and handle them in a timely manner. - Others: There are risky incidents that are marked as medium-risk, low-risk, and informational alerts detected in your systems, and you should view details about results of compliance checks and take necessary actions. • To quickly view details of top 5 abnormal compliance risks discovered for the last 30 days, click the Abnormal Baseline Settings panel. <ul style="list-style-type: none"> - You can view details of the top compliance risks discovered in the latest check, such as check item name, severity, asset name, and discovery time. - If no data is available, no violations are detected for the last 30 days.

Your Security Score over Time

SecMaster displays your security scores for the last 7 days.

Figure 4-3 Your Security Score over Time



4.2 Security Score

SecMaster displays the overall security assessment results of your assets on the cloud in real time and evaluates your overall asset security health score.

This topic describes how your security score is calculated.

Security Score

SecMaster evaluates the over security posture of your assets based on the SecMaster edition you are using.

- There are five risk severity levels, **Secure**, **Informational**, **Low**, **Medium**, **High**, and **Critical**.
- The score ranges from 0 to 100. The higher the security score, the lower the risk severity level.
- The security score starts from **0** and the risk severity level is escalated up from **Secure** to the next level every 20 points. For example, for scores ranging from **40** to **60**, the risk severity is **Medium**.
- The color keys listed on the right of the chart show the names of donut slices. Different color represents different risk severity levels. For example, the yellow slice indicates that your asset risk severity is **Medium**.
- The security score is updated in real time when you refresh status of the alert incident after risk handling.

NOTE

After risks are fixed, manually ignore or handle alert incidents and update the alert incident status in the alert list. The risk severity can be down to a proper level accordingly.

Table 4-2 Security score table

Severity	Security Score	Description
Secure	100	Congratulations. Your assets are secure.
Informational	$80 \leq \text{Security Score} < 100$	Your system should be hardened as several security risks have been detected.
Low	$60 \leq \text{Security Score} < 80$	Your system should be hardened in a timely manner as too many security risks have been detected.
Medium	$40 \leq \text{Security Score} < 60$	Your system should be hardened, or your assets will be vulnerable to attacks.
High	$20 \leq \text{Security Score} < 40$	Detected risks should be handled immediately, or your assets will be vulnerable to attacks.
Critical	$0 \leq \text{Security Score} < 20$	Detected risks should be handled immediately, or your assets may be attacked.

Unscored Check Items

[Table 4-3](#) lists the security check items and corresponding points.

Table 4-3 Unscored check items

Category	Unscored Item	Points	Suggestion	Maximum Unscored Point
Enabling of security services	Security-related services not enabled	-	Enable security-related services.	30
Compliance Check	Critical non-compliance items not fixed	10	Fix compliance violations by referring recommended fixes and start a scan again. The security score will be updated.	20
	High-risk non-compliance items not fixed	5		
	Medium-risk non-compliance items not fixed	2		
	Low-risk non-compliance items not fixed	0.1		
Vulnerabilities	Critical vulnerabilities not fixed	10	Fix vulnerabilities by referring corresponding suggestions and start a scan again. The security score will be updated.	20
	High-risk vulnerabilities not fixed	5		
	Medium-risk vulnerabilities not fixed	2		
	Low-risk vulnerabilities not fixed	0.1		
Threat Alerts	Critical alerts not fixed	10	Fix the threats by referring to the suggestions. The security score will be updated accordingly.	30
	High-risk alerts not fixed	5		
	Medium-risk alerts not fixed	2		
	Low-risk alerts not fixed	0.1		

5 Workspaces

5.1 Workspace Overview

This section describes the definition, types, and basic operations of workspaces.

What Is a Workspace?

Workspaces are operation platforms of SecMaster resources. A single workspace can be bound to common projects and enterprise projects for different application scenarios.

What Is a Data Space?

A data space is a unit for data grouping, load balancing, and flow control. Data in the same data space shares the same load balancing policy.

What Is a Data Pipeline?

A data transfer message topic and a storage index form a pipeline.

General Rules for Workspaces

- A maximum of five workspaces can be created under a single account in a region.
- A maximum of five data spaces can be created in a workspace.
- A maximum of 20 pipelines can be created in a data space.

5.2 Creating a Workspace

Workspaces are operation platforms of SecMaster resources. A single workspace can be bound to common projects and enterprise projects for different application scenarios.

Before using functions such as security analysis and data consumption, you need to create a workspace to divide resources into different working scenarios. This makes your resources easier for search and use.

This section describes how to create a workspace.

Limitations and Constraints

A maximum of five workspaces can be created under a single account in a region.

Procedure


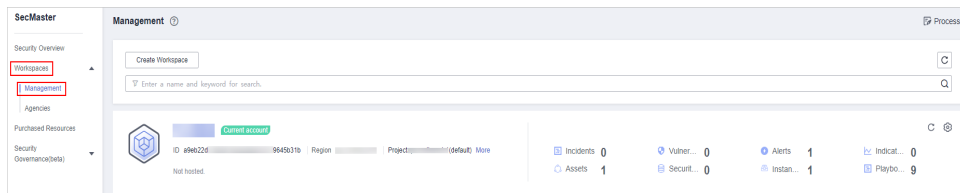
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**.

Figure 5-1 Workspaces



- Step 4** On the **Management** page, click **Create Workspace**. The **Create Workspace** slide-out panel is displayed.

Figure 5-2 Create Workspace

The screenshot shows the 'Create Workspace' slide-out panel. It contains the following fields and options:

- Region:** A dropdown menu with a search icon.
- Enterprise Project:** A dropdown menu.
- Workspace Name:** A text input field with a red asterisk. Below it, there are two bullet points:
 - The value can contain Chinese characters, uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and special characters (-, _).
 - The length cannot exceed 64 characters.
- Tag:** A text input field.
- Description:** A larger text input area.

- Step 5** Configure workspace parameters by referring to the following table.

Table 5-1 Creating a workspace

Parameter	Description
Region	Select the region where you want to add the workspace.

Parameter	Description
Enterprise Project	Select an enterprise project from the drop-down list. This option is only available if you have logged in using an enterprise account, or if you have enabled enterprise projects. NOTE Value default indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project.
Workspace Name	Specify a name for your workspace. It must meet the following requirements: <ul style="list-style-type: none"> • Only letters (A to Z and a to z), numbers (0 to 9), and the following special characters are allowed: -_() • A maximum of 64 characters are allowed.
Tag	(Optional) Tag of the workspace, which is used to identify the workspace and help you classify and track your workspaces.
Description	(Optional) User remarks

Step 6 Click **OK**.

----End


5.3 Managing Workspaces

5.3.1 Viewing Workspace Details

This section describes how to view information about a workspace, including the name, type, and creation time.

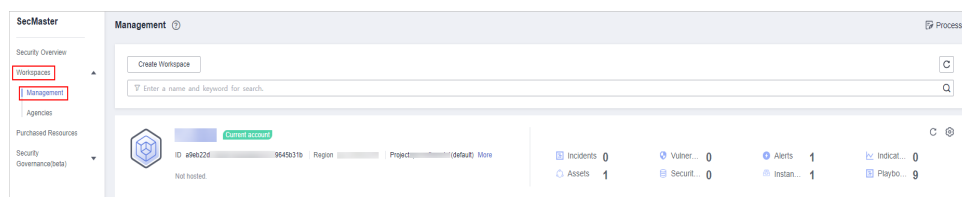
Viewing a Workspace

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

Step 3 In the navigation pane, choose **Workspaces > Management**.

Figure 5-3 Workspaces



Step 4 On the **Management** page, view information about existing workspaces.


If there are many workspaces, you can enter a keyword in the search box and click  to quickly find the one you want.

Figure 5-4 Workspace details

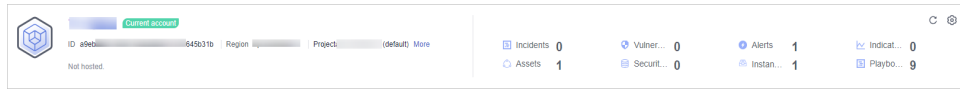


Table 5-2 Workspace parameters

Parameter	Description
Workspace Name	Name of the workspace
Workspace Type	Type of the workspace.
ID	ID of the workspace
Region	Region to which the workspace belongs
Project	Project to which the workspace belongs
More	Workspace details
Incidents	Number of incidents in the workspace
Vulnerabilities	Number of vulnerabilities in the workspace
Alerts	Number of alerts in the workspace
Indicators	Number of indicators in the workspace
Assets	Number of assets in the workspace
Security Analysis	Number of existing data spaces in the workspace
Instances	Number of instances in the workspace
Playbooks	Number of playbooks in the workspace


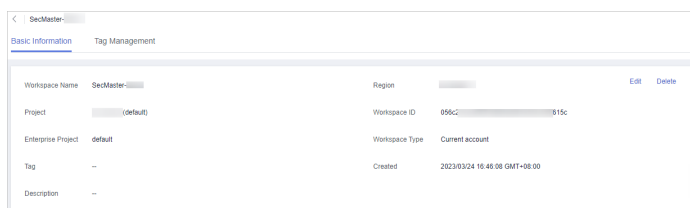
Step 5 To view details about a workspace, click  on the right of the workspace. The workspace details page is displayed.

Figure 5-5 Basic workspace information




----End

5.3.2 Editing a Workspace

After a workspace is added, you can modify the workspace name, tag, and description. This section describes how to edit a workspace.

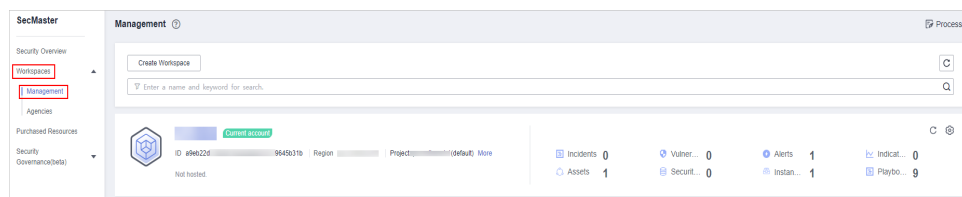
Editing a Workspace

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

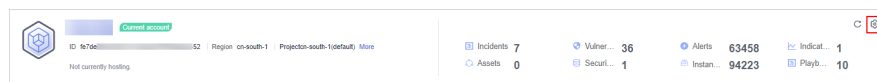
Step 3 In the navigation pane, choose **Workspaces > Management**.

Figure 5-6 Workspaces



Step 4 Click  on the right of the workspace. The workspace details page is displayed.

Figure 5-7 Workspace details page



Step 5 On the **Basic Information** tab page displayed, click **Edit**.

Step 6 Edit the workspace name, tag, or description and click **Save**.

----End

5.3.3 Deleting a Workspace

This section describes how to delete a workspace that is no longer needed.


After a workspace is deleted, assets in the workspace will face risks. Deleted workspaces cannot be restored. Exercise caution when performing this operation.

Limitations and Constraints

- When you delete a workspace, the playbooks, workflows, and engines running in it stop immediately.
- If you select **Permanently delete the workspace**, all content in the workspace will be permanently deleted and cannot be restored.

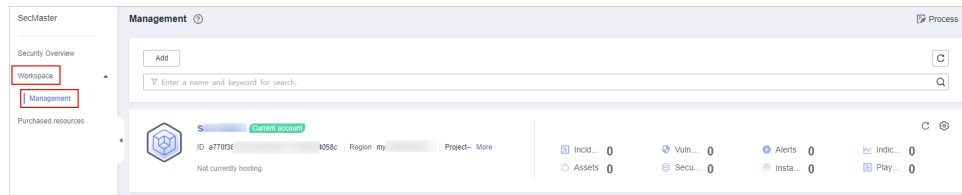
Deleting a Workspace

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

Step 3 In the navigation pane, choose **Workspaces > Management**.

Figure 5-8 Workspaces




Step 4 Click  next to the workspace you want to delete.

Figure 5-9 Workspace details page



Step 5 On the **Basic Information** tab page displayed, click **Delete**.

Step 6 On the **Delete Workspace** page is displayed, confirm the information, select **Permanently delete the workspace**, and enter the workspace name in the **Confirm Deletion** text box.

 **CAUTION**

- When you delete a workspace, the playbooks, workflows, and engines running in it stop immediately.
 - If you select **Permanently delete the workspace**, all content in the workspace will be permanently deleted and cannot be restored.
-

Step 7 Click **Delete** in the lower right corner of the page.


----End

6 Viewing Purchased Resources

You can view resources owned by the current account on the **Purchased Resources** page and manage them centrally.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

Step 3 In the navigation pane on the left, choose **Purchased Resources**.

Step 4 View details on the purchased resource page.

- Overview
 - Total/Subscribed Regions: displays regions where SecMaster is enabled in the current account.
 - Upgradeable: displays the number of applied resources that can be upgraded in the current account.
 - Versions About to Expire: Displays the number of SecMaster editions and value-added packages that are about to expire.
 - Total Quota: displays the quota of applied resources in the current account.
- Details about SecMaster resources you applied in each region.

----End

7 Security Situation

7.1 Situation Overview

The **Situation Overview** page displays the security evaluation of resources in the current workspace in real time. On the **Security Overview** page, you can view security status of your cloud resources and manage risks centrally.

Procedure


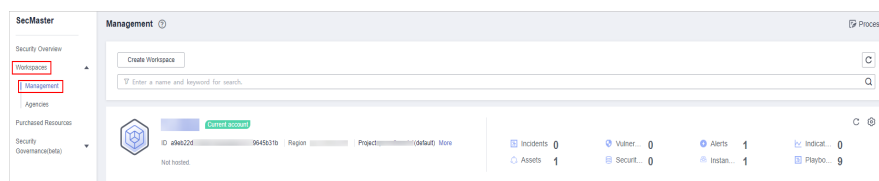
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-1 Management



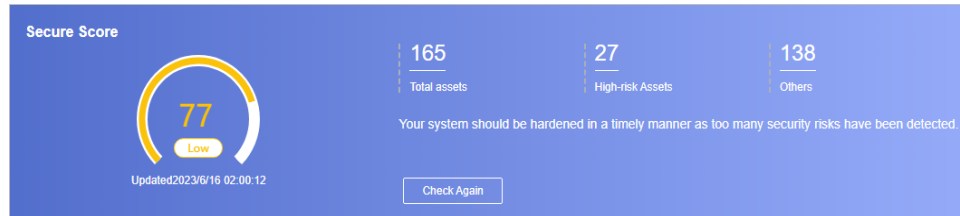
- Step 4** In the navigation pane on the left, choose **Security Situation > Situation Overview**.
- Step 5** On the **Security Overview** page, you can view the security overview of your assets and perform related operations. The **Situation Overview** page consists of the following modules:
 - [Security Score](#)
 - [Security Monitoring](#)
 - [Your Security Score over Time](#)

----End

Security Score

The security score shows the overall health status of your workloads on the cloud so you can quickly learn of unhandled risks and their threats to your assets.

Figure 7-2 Security Score



- The score ranges from 0 to 100. The higher the security score, the more secure your assets. For details, see [Security Scores and Unscored Items](#).
- Different color blocks in the security score ring chart indicate different severity levels. For example, yellow indicates that your security is medium.
- Click **Handle Now**. The **Risks** pane is displayed on the right. You can handle risks by referring to the corresponding guidance.
 - The **Risks** slide-out panel lists all threats that you should handle in a timely manner. These threats are included in the **Threat Alarms**, **Vulnerabilities**, and **Abnormal Baseline Settings** areas.
 - The **Risks** pane displays the latest check results of the last scan. The **Alerts**, **Vulnerabilities**, and **Abnormal Baseline Settings** pages show check results of all previous scans. So, you will find the threat number on the **Risks** pane is less than that on those pages. You can click **Handle** for an alert on the **Risks** pane to go to the corresponding page quickly.
 - **Handling detected security risks:**
 - In the **Security Score** area, click **Handle Now**.
 - On the **Risks** slide-out panel displayed, click **Handle**.
 - On the page displayed, handle risk alerts, vulnerabilities, or baseline inspection items.
- The security score is updated when you refresh status of the alert incident after risk handling. After you fix the risks, you can click **Check Again** so that SecMaster can check and score your system again.

NOTE

- After risks are fixed, manually ignore or handle alert incidents and update the alert incident status in the alert list. The risk severity can be down to a proper level accordingly.
- The security score reflects the security situation of your system last time you let SecMaster check the system. To obtain the latest score, click **Check Again**.

Security Scores and Unscored Items

SecMaster assesses the overall security situation of your assets in real time and scores your assets based on the SecMaster edition and features you are using.

This section describes how your security score is calculated.

- Security Score

SecMaster evaluates the overall security situation of your assets.

 - There are five risk severity levels, **Secure**, **Informational**, **Low**, **Medium**, **High**, and **Critical**.
 - The score ranges from 0 to 100. The higher the security score, the lower the risk severity level.
 - The security score starts from **0** and the risk severity level is escalated up from **Secure** to the next level every 20 points. For example, for scores ranging from **40** to **60**, the risk severity is **Medium**.
 - The color keys listed on the right of the chart show the names of donut slices. Different color represents different risk severity levels. For example, the yellow slice indicates that your asset risk severity is **Medium**.
 - The security score is updated in real time when you refresh status of the alert incident after risk handling.

 **NOTE**

After risks are fixed, manually ignore or handle alert incidents and update the alert incident status in the alert list. The risk severity can be down to a proper level accordingly.

Table 7-1 Security score table

Severity	Security Score	Description
Secure	100	Congratulations. Your assets are secure.
Informational	80 ≤ Security Score < 100	Your system should be hardened as several security risks have been detected.
Low	60 ≤ Security Score < 80	Your system should be hardened in a timely manner as too many security risks have been detected.
Medium	40 ≤ Security Score < 60	Your system should be hardened, or your assets will be vulnerable to attacks.
High	20 ≤ Security Score < 40	Detected risks should be handled immediately, or your assets will be vulnerable to attacks.
Critical	0 ≤ Security Score < 20	Detected risks should be handled immediately, or your assets may be attacked.

- Unscored Check Items

Table 7-2 lists the security check items and corresponding points.

Table 7-2 Unscored check items

Category	Unscored Item	Points	Suggestion	Maximum Unscored Point
Enabling of security services	Security-related services not enabled	-	Enable security-related services.	30
Compliance Check	Critical non-compliance items not fixed	10	Fix compliance violations by referring recommended fixes and start a scan again. The security score will be updated.	20
	High-risk non-compliance items not fixed	5		
	Medium-risk non-compliance items not fixed	2		
	Low-risk non-compliance items not fixed	0.1		
Vulnerabilities	Critical vulnerabilities not fixed	10	Fix vulnerabilities by referring corresponding suggestions and start a scan again. The security score will be updated.	20
	High-risk vulnerabilities not fixed	5		
	Medium-risk vulnerabilities not fixed	2		
	Low-risk vulnerabilities not fixed	0.1		
Threat Alerts	Critical alerts not fixed	10	Fix the threats by referring to the suggestions. The security score will be updated accordingly.	30
	High-risk alerts not fixed	5		
	Medium-risk alerts not fixed	2		
	Low-risk alerts not fixed	0.1		

Security Monitoring

The **Security Monitoring** area includes **Threat Alarms**, **Vulnerabilities**, and **Abnormal Baseline Settings**, which sort risks that have not been handled.

Figure 7-3 Security Monitoring

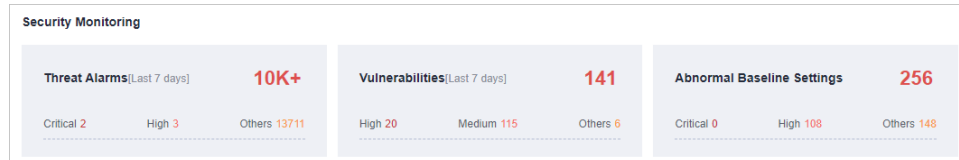


Table 7-3 Security Monitoring parameters

Parameter	Description
Threat Alarms	<p>This panel displays the unhandled threat alerts for the last 7 days. You can quickly learn of the total number of unhandled threat alerts and the number of vulnerabilities at each severity level.</p> <ul style="list-style-type: none"> • Risk severity levels: <ul style="list-style-type: none"> – Critical: There are intrusions to your workloads, and you should view alert details and handle the alert in a timely manner. – High: There are abnormal incidents on your workloads, and you should view alert details and handle the alert in a timely manner. – Others: There are risky incidents that are marked as medium-risk, low-risk, and informational alerts detected in your systems, and you should view alert details and take necessary actions. • To quickly view details of top 5 threat alerts for the last 7 days, click the Threat Alarms panel. <ul style="list-style-type: none"> – You can view details of those threats, including the threat alert name, severity, asset name, and discovery time. – If no data is available here, no threat alerts are generated for the last 7 days. – You can click View More to go to the Alerts page and view more alerts. You can also customize filter criteria to query alert information.

Parameter	Description
Vulnerabilities	<p>This panel displays the top five vulnerability types and the total number of unfixed vulnerabilities in your assets for the last 7 days. You can quickly learn of the total number of unfixed vulnerabilities and the number of vulnerabilities at each severity level.</p> <ul style="list-style-type: none"> ● Risk severity levels: <ul style="list-style-type: none"> - High: There are vulnerabilities on your workloads, and you should view vulnerability details and handle them in a timely manner. - Medium: There are abnormal incidents on your workloads, and you should view vulnerability details and handle the vulnerability in a timely manner. - Others: There are risky incidents that are marked as low-risk or informational in your systems, and you should view vulnerability details and take necessary actions. ● When you click the Top 5 Vulnerability Types tab, the system displays top 5 vulnerability types. <ul style="list-style-type: none"> - Vulnerability rankings are based on the number of hosts a vulnerability affects. The vulnerability ranked the first affects the most hosts. - The data is displayed in Top 5 Vulnerability Types only when the hosts have Host Security Service (HSS) Agent version 2.0 installed. If no data is displayed or you want to view top 5 vulnerability types, upgrade Agent from 1.0 to 2.0. ● Click Top 5 Real-Time Vulnerabilities tab. The system displays the top 5 vulnerability incidents for the last 7 days. You can quickly view vulnerability details. <ul style="list-style-type: none"> - You can view details such as the vulnerability name, severity, asset name, and discovery time. - If no data is available here, no vulnerabilities are detected on the current day. - You can click View More to go to the Vulnerabilities page and view more vulnerabilities. You can also customize filter criteria to query vulnerability information.

Parameter	Description
Abnormal Baseline Settings	<p>This panel displays the total number of compliance violations detected for the last 30 days. You can quickly learn of total number of violations and the number of violations at each severity level.</p> <ul style="list-style-type: none"> ● Risk severity levels: <ul style="list-style-type: none"> - Critical: There are intrusions to your workloads, and you should view details about compliance risks and handle them in a timely manner. - High: There are abnormal incidents on your workloads, and you should view details about compliance risks and handle them in a timely manner. - Others: There are risky incidents that are marked as medium-risk, low-risk, and informational alerts detected in your systems, and you should view details about compliance risks and take necessary actions. ● To quickly view details of top 5 abnormal compliance risks discovered for the last 30 days, click the Abnormal Baseline Settings panel. <ul style="list-style-type: none"> - You can view details of the top compliance risks discovered in the latest check, such as check item name, severity, asset name, and discovery time. - If no data is available, no compliance violations are detected for the last 30 days. - You can click View More to go to the Baseline Inspection page and view more compliance risks. You can also customize filter criteria to make an advanced search.

Your Security Score over Time

SecMaster displays your security scores **over the last 7 days**.

Figure 7-4 Your Security Score over Time



7.2 Large Screen

7.2.1 Overall Situation Screen

There are always such scenarios as presentation, reporting, or real-time monitoring where you need to present the analysis results of SecMaster on big screens to achieve better demonstration effect. It is not ideal to just zoom in the console. Now, SecMaster **Large Screen** is a good choice for you to display the service console on bigger screens for a better visual effect.

By default, SecMaster provides a large screen for comprehensive situation awareness by displaying the attack history, attack status, and attack trend. This allows you to manage security incidents before, when, and after they happen.

Procedure


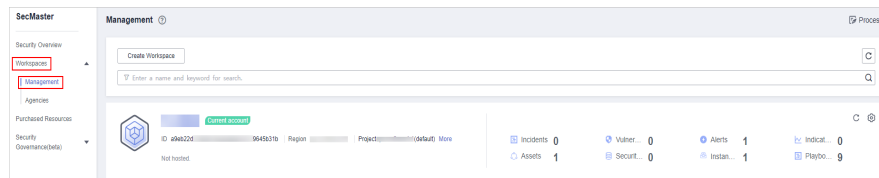
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-5 Management



- Step 4** In the navigation pane on the left, choose **Security Situation > Large Screen**.
- Step 5** Click the **Overall Situation** screen. The large screen for overall situation awareness is displayed.

This screen includes many graphs.

----End

Security Score

The security and health scores of the current asset are displayed.

- There are five risk severity levels, **Secure**, **Informational**, **Low**, **Medium**, **High**, and **Critical**.
- The score ranges from 0 to 100. The higher the security score, the lower the risk severity level.
- The security score starts from **0** and the risk severity level is escalated up from **Secure** to the next level every 20 points. For example, for scores ranging from **40** to **60**, the risk severity is **Medium**.

- The color keys listed on the right of the chart show the names of donut slices. Different color represents different risk severity levels. For example, the yellow slice indicates that your asset risk severity is **Medium**.

Alert Statistics

The alert statistics of interconnected services are displayed.

- **New Alerts:** Displays the total number of new alerts generated on the current day.
- **Alerts:** Displays the number of threat alerts in the last seven days.
- **Unhandled Alerts:** displays the number of alerts to be handled in the last seven days.
- **Handled Alerts:** displays the number of alerts that have been cleared in the last seven days.

Asset Protection

The protection status of hosts and websites is displayed, including the proportion of protected and unprotected assets. You can move the mouse pointer to a module to view the number of protected/unprotected assets.

Baseline Inspection

The fixing status of the baseline configuration and vulnerabilities of your assets, distribution of risky resources, and vulnerability fixing trend within seven days are displayed.

- **Baseline Settings:** displays the numbers of passed and failed baseline settings based on the last baseline inspection.
- **Vulnerabilities:** Displays the numbers of fixed and unfixed vulnerabilities based on vulnerabilities found in the baseline checks in the last seven days.
- **Resources by Severity:** displays the number of vulnerable resources by severity based on the last baseline inspection. **Severity: Critical, High, Medium, Low, and Info.**
- **Vulnerabilities [Last 7 Days]:** Displays the vulnerability distribution trend of services covered in baseline inspection in the last seven days.

Recent Threats

The number of threatened assets and log access volume in the last seven days are displayed. The horizontal coordinate of the threat posture indicates the time, the left vertical coordinate indicates the number of threatened assets, and the right vertical coordinate indicates the number of threatened access logs. Hover the cursor over a date to view the number of threatened assets of that day.

To-Dos

The tickets pending processing in the current workspace are displayed.

Resolved Issues

The alert handling information and SLA and MTTR fulfillment rates and automatic handling statistics in the last seven days are displayed.

- **Alerts:** displays the total number of alerts of interconnected services.
- **Handled:** displays the total number of alerts that have been closed in the last seven days.
- **Manual:** displays the total number of alerts that are handled in a timely manner, that is, the total number of alerts that are handled within the SLA time set for alerts.
- **Auto:** displays the total number of alerts that are automatically handled and closed by the playbook.
- **SLA and MTTR [Last 7 Days]:** displays the alert handling SLA statistics and average MTTR response time in the last seven days.
 - **SLA Statistics:** displays the alert handling timeliness in the last 7 days. The formula is as follows:

For an alert for which the SLA field has been set, if the alert closure incident minus the alert generation time is less than or equal to the configured SLA time, the requirement is met. Otherwise, the requirement is not met.
 - **MTTR (s):** indicates the average alert closure time in the 7 seven days. The formula is as follows:

$$\text{MTTR} = \text{Total processing time of each alert} / \text{Total number of alerts.}$$
$$\text{Processing time of each alert} = \text{Closure time} - \text{Creation time.}$$
- **Handled Incidents [Last 7 Days]:** displays the total number of alerts that have been automatically processed by playbooks in the last seven days.

7.2.2 Monitoring Statistics Screen

There are always such scenarios as presentation, reporting, or real-time monitoring where you need to present the analysis results of SecMaster on big screens to achieve better demonstration effect. It is not ideal to just zoom in the console. Now, SecMaster **Large Screen** is a good choice for you to display the service console on bigger screens for a better visual effect.

By default, SecMaster provides a **Monitoring Statistics** screen. You can view the overview of unhandled alerts, incidents, vulnerabilities, and baseline settings on one screen.

Procedure


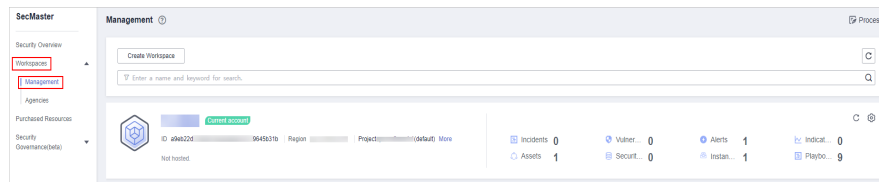
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-6 Management



Step 4 In the navigation pane on the left, choose **Security Situation > Large Screen**.

Step 5 Click the **Monitoring Statistics** image to go to the corresponding large screen page.

This screen includes many graphs.

----End

Monitoring Statistics Overview

This screen displays the total number of unhandled alerts, incidents, vulnerabilities, and unsafe baseline settings.

Unhandled Alerts

The table lists information about top 5 unhandled threat alerts, including the alert discovery time, alert description, alert severity, and alert type.

These top 5 alerts are sorted by generation time with the latest one placed at the top.

Unhandled Incidents

The table lists information about the top 5 unhandled incidents, including the incident discovery time, description, severity, and type.

These top 5 incidents are sorted by generation time with the latest one placed at the top.

Unhandled Vulnerabilities

The table lists information about the top 5 unhandled vulnerabilities, including the discovery time, description, type, severity, and number of affected assets.

These top 5 vulnerabilities are sorted by discovery time with the latest one placed at the top.

Unhandled Baseline Settings

This table lists information about the top 5 unhandled unsafe baseline settings, including the discovery time, description, check method, and total number of vulnerable resources.

These top 5 unhandled baseline settings are sorted by discovery time with the latest one placed at the top.

7.2.3 Asset Security Screen

There are always such scenarios as presentation, reporting, or real-time monitoring where you need to present the analysis results of SecMaster on big screens to achieve better demonstration effect. It is not ideal to just zoom in the console. Now, SecMaster **Large Screen** is a good choice for you to display the service console on bigger screens for a better visual effect.

By default, SecMaster provides an asset screen for you. With this screen, you will learn about overall information about your assets at a glance, including how many assets you have, how many of them have been attacked, and how many of them are unprotected.

Procedure


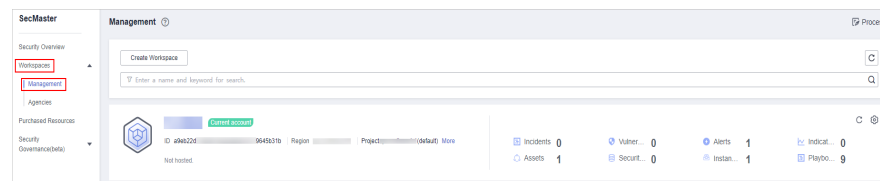
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-7 Management



- Step 4** In the navigation pane on the left, choose **Security Situation > Large Screen**.
- Step 5** Click the **Asset Security** image to go to the large screen for assets.

This screen includes many graphs.

----End

Asset Security Screen Overview

On this screen, you can view the total numbers of assets, attacked assets, unprotected assets, vulnerabilities, and assets with unsafe settings.

- **Assets:** total number of assets in the current workspace of the current account.
- **Attacked Assets:** total number of assets with alerts in the current workspace of the current account.
- **Unprotected Assets:** total number of unprotected assets in the current workspace of the current account. For example, if you have not enabled HSS for some ECSs, the number of them will be displayed here.
- **Vulnerabilities and assets with unsafe settings:** the total number of assets that have vulnerabilities, unhandled insecure baseline settings, or have not been protected in the current workspace of the current account. This number does not count duplicate assets.

Asset Distribution

In this area, you can view assets by type, asset protection rate, asset change trend, and distribution of the five assets attacked most.

- **Assets by Type:** displays the distribution of different asset types in the current workspace of the current account.
- **Protection by Asset Type (%):** displays the protection rates of different asset types in the current workspace of the current account.
- **Asset Changes:** displays the changes in total assets and vulnerable assets in the current workspace of the current account over the last seven days.
- **Top 5 Attacked Assets:** displays the top 5 attacked assets in the current workspace of the current account and the number of attacks.

Top 5 Assets with the Most Vulnerabilities and Top 5 Departments with the Highest Protection Rate

In this area, you will see the five assets with the most vulnerabilities and the five departments with the highest protection rate.

- **Top 5 Assets with the Most Vulnerabilities:** displays the five assets with the most vulnerabilities, including the asset IP address, department, and number of vulnerabilities in real time.
- **Top 5 Departments with the Highest Protection Rate:** includes the protection rates of asset type, department, WAF, HSS, and vulnerability fix.

The top 5 departments are sorted based on the protection rate. The department with the lowest protection rate is ranked first.

7.2.4 Threat Situation Screen

There are always such scenarios as presentation, reporting, or real-time monitoring where you need to present the analysis results of SecMaster on big screens to achieve better demonstration effect. It is not ideal to just zoom in the console. Now, SecMaster **Large Screen** is a good choice for you to display the service console on bigger screens for a better visual effect.

By default, SecMaster provides a threat situation screen, which shows how many network attacks, application-layer attacks, and server-layer attacks against your assets over the last seven days.

Procedure

- Step 1** Click the **Threat Situation** image to go to the information page.

This screen includes many graphs.

----End

Threat Situation screen

This area displays the number of attacks by types, including network, application, and server attacks.

- **Network Attacks:** indicates the total number of attacks at the network layer in the last 7 days. You can view network attacks by the day and changes in attack quantity compared to the last 7 days.
- **Application Attacks:** indicates the total number of attacks at the application layer in the last 7 days. You can view application attacks by the day and changes in attack quantity compared to the last 7 days.
- **Server Attacks:** indicates the total number of attacks against servers in the last 7 days. You can view server attacks by the day and changes in attack quantity compared to the last 7 days.

Attack Source Distribution

This graph displays the five attack sources who launched the most attacks against the network and application layers. You will see attacked asset details, including IP addresses, departments, and quantity.

- **Top 5 Network Attack Sources:** displays the five IP addresses from where originate the most network attacks, including geographical locations and the number of alerts, in the last 7 days.
- **Top 5 Application Attack Sources:** displays the five source IP addresses for which the most application attack alerts have been reported, including geographical locations and the number of alerts, in the last 7 days.

Attacks by Type

This graph shows top 5 network attack types, top 5 application attack types, and server attack types.

- **Top 5 Network Attack Types:** indicates the 5 network attack types with the most alerts generated in the last 7 days.
- **Top 5 Application Attack Types:** indicates the 5 application attack types with the most alerts generated in the last 7 days.
- **Top 5 Server Attack Types:** indicates the 5 server attack types with the most alerts generated in the last 7 days.

Threat Situation Statistics

This graph shows the statistics about alerts, logs, and threat detection models in the current account.

- **Alert Statistics**
 - **Logs:** indicates the total number of incoming logs in the last 7 days.
 - **Threats:** indicates the total number of DDoS, network, application, and server attacks in the last 7 days.
 - **Alerts:** total number of generated over the last 7 days.
 - **Incidents:** total number of incidents over the last 7 days.
- **Log Analysis**
 - **Log volume:** total log storage volume, in KB, MB, or GB.
 - **Log volume comparison:** indicates log volume changes by percentage since the previous 7-day cycle. Calculation method: [(Number of logs for

- this cycle – Number of logs for the previous cycle)/Number of logs for the previous cycle] x 100%.
- **Log Analysis:** displays the five log sources that report the most logs over the last 7 days.
- Model Statistics
 - **Models:** total number of alert models.
 - **Threats by Model:** displays the 10 alert models that generate the most alerts over the last 7 days as well as how many alerts they report.

7.2.5 Vulnerable Assets Screen

There are always such scenarios as presentation, reporting, or real-time monitoring where you need to present the analysis results of SecMaster on big screens to achieve better demonstration effect. It is not ideal to just zoom in the console. Now, SecMaster **Large Screen** is a good choice for you to display the service console on bigger screens for a better visual effect.

By default, SecMaster provides a vulnerable asset screen. With this screen, you can view the overview of vulnerable assets, asset vulnerabilities, unsafe baseline settings, and unprotected assets.

Procedure


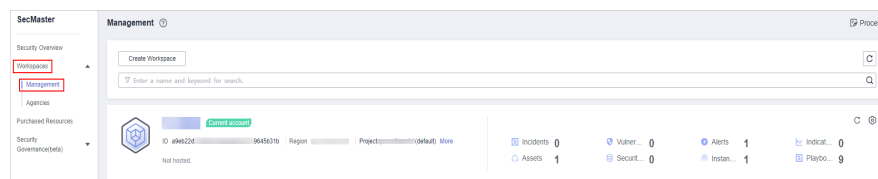
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-8 Management



- Step 4** In the navigation pane on the left, choose **Security Situation > Large Screen**.
- Step 5** Click the **Vulnerable Assets** image to go to the information page.

This screen includes many graphs.

----End

Vulnerable Assets Overview

This graph displays the total numbers of vulnerable assets, vulnerabilities, unsafe baseline settings, and unprotected assets.

Vulnerable assets refer to assets with unhandled vulnerabilities or unsafe baseline settings and assets that are not under protection at the current time.

Top 5 Departments with the Most Vulnerabilities

This graph shows the five departments with the most vulnerabilities. You will view the details of these departments, including the department name, number of vulnerable assets, number of unfixed vulnerabilities, and number of unprotected assets.

Top 5 Department with the Most Unprotected Assets

This graph displays the 5 departments with the most failed protection policies. You can view the details about these departments, including the department name and what protection policies they failed, such as DBSS, WAF, Anti-DDoS, HSS, and CFW

The graph displays the five departments with the most unprotected assets.

Vulnerability Fix Rate

This graph shows the vulnerability fix rate, top 5 vulnerability types, and vulnerability trend changes.

- **Vulnerability Fix Rate:** the rates of fixed high-risk, medium-risk, low-risk, and informational vulnerabilities.
- **Top 5 Vulnerability Types:** the types and number of top 5 vulnerabilities.
- **Vulnerability Changes:** changes in the number of high-risk, medium-risk, low-risk, and informational vulnerabilities over the past 7 days.

Baseline Inspection Pass Rate

You can learn about baseline inspection results at a glance, including the pass rate, what resources have failed the inspection, failed checks, resource types, and the number of total check items.

7.3 Reports


7.3.1 Creating or Copying a Report

SecMaster provides you with security reports. You can create a security report template so that you can learn of your resource security status in a timely manner.

This section describes how to create a security report and how to quickly create a security report by copying an existing template.

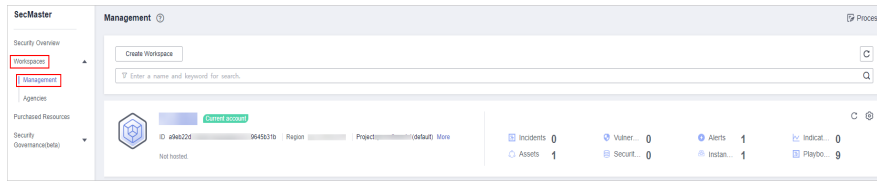
Creating a Report

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

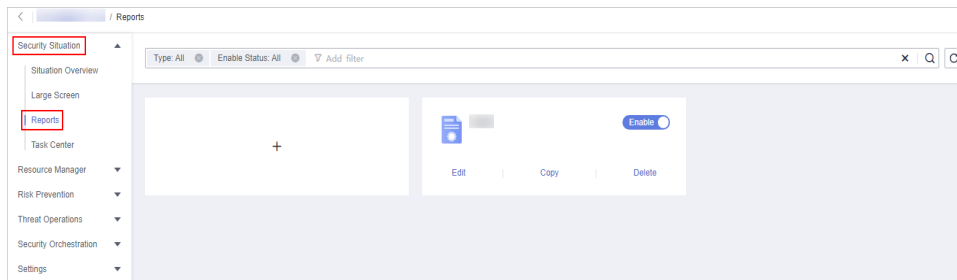
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-9 Management



Step 4 In the navigation pane on the left, choose **Security Situation > Reports**.

Figure 7-10 Reports



Step 5 On the **Reports** page, click **+** to go to the basic configuration page.

Step 6 Configure basic information of the report.

Table 7-4 Report parameters

Parameter	Description
Report Name	Name of the report you want to create.
Schedule	Select a report schedule. <ul style="list-style-type: none"> Daily: SecMaster collects security information from 0:00 to 24:00 of the previous day by default. Weekly: SecMaster collects security information from 00:00 on Monday to 24:00 on Sunday of the previous week. Monthly: SecMaster collects security information from 00:00 on the first day to 24:00 on the last day of the previous month.
Data Scope	Reports will be generated for the time range you specify.

Step 7 Click **Next: Report Choose** in the upper right corner. The **Report Selection** page is displayed.

Step 8 In the existing report layout area on the left, select a report layout. After selecting, you can preview the report layout in the right pane.

Step 9 Click **Complete** in the lower right corner. On the displayed **Reports** page, view the created report.

----End

Copying a Report


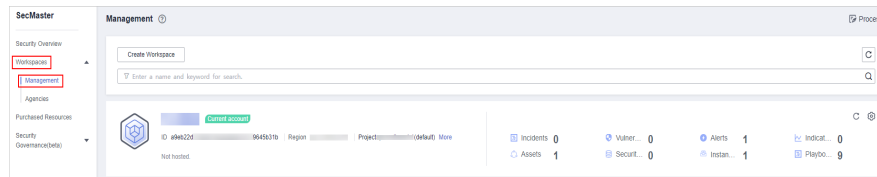
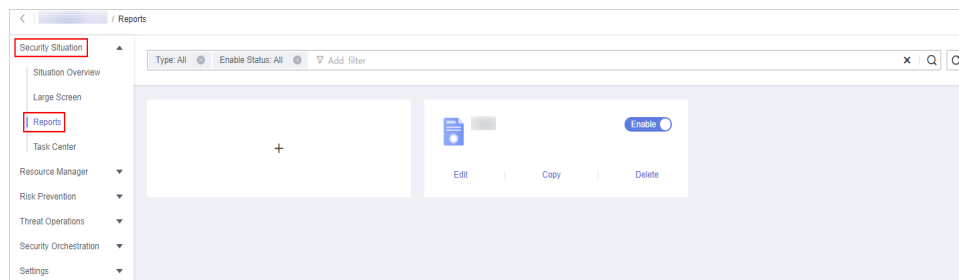
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-11 Management



- Step 4** In the navigation pane on the left, choose **Security Situation > Reports**.

Figure 7-12 Reports



- Step 5** Select a report template and click **Copy**.
- Step 6** Edit basic information of the report.
- Step 7** Click **Next: Report Choose**. The report configuration page is displayed.
- Step 8** Click **Complete** in the lower right corner. On the displayed **Reports** page, view the newly created report.

----End

7.3.2 Viewing a Security Report

View a created security report and its displayed information.

Procedure


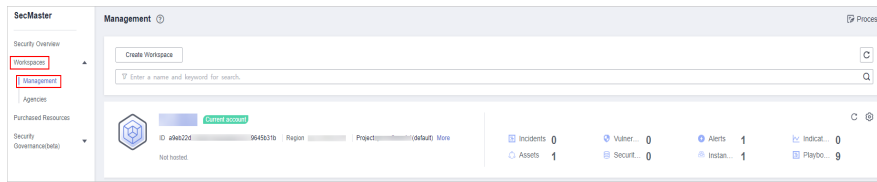
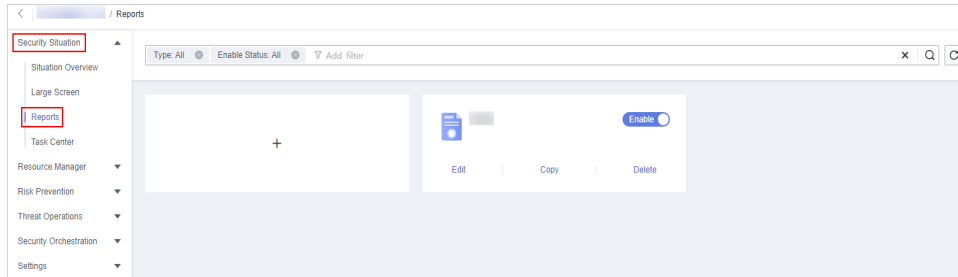
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-13 Management




Step 4 In the navigation pane on the left, choose **Security Situation > Reports**.

Figure 7-14 Reports



Step 5 Select the target report and click the report icon. The report details page is displayed.

On the report details page, you can preview details about the current security report.

When there are a large number of reports, you can search for a specific report type by selecting the **Type** or **Enabling Status** of the report, and then click .

----End

Content in the Daily Report Template

- **Data Scope**
The default data scope of a daily report is from 00:00:00 to 23:59:59 on the previous day.
- **Security score**
SecMaster evaluates and scores your asset security for the previous day (from 00:00:00 to 23:59:29) so that you can quickly learn of the overall security posture of assets. This score varies depending on the SecMaster edition you are using.
- **Baseline check**
Displays the statistics of the latest baseline inspection, including the total number of current baseline check items, number of compliance check items, number of failed compliance check items, and proportion of failed compliance check items.
- **Security vulnerabilities**
Displays the vulnerability statistics of the accessed cloud service on the previous day, including the total number of vulnerabilities, and number of unfixed vulnerabilities.
- **Policy coverage**

Displays the coverage of current security products, including the following information: number of instances protected by security products (= number of protected ECSs + number of protected WAF instances), host security coverage (= number of protected ECSs/total number of ECSs), number of current protected ECSs, and number of current protected websites.

- **Asset security**

Displays the security status of current assets, including the total number of assets you have, and the number of vulnerable assets.

- Security analysis

Displays security analysis statistics of the previous day, including the total security log traffic of the previous day, and the number of security log models.

- Security response

Displays the security response status of the previous day, including the total number of alerts handled, intrusions confirmed, and playbooks executed, percentage of alerts automatically handled by playbooks, average MTTR, and number of confirmed high-risk intrusions for the previous day.

- **Asset risk**

Displays the asset security status of **the previous day**, including number of attacked assets, number of unprotected assets, number of vulnerable assets, and asset protection rate of the previous day, as well as the asset changes over the **last 7 days**.

- **Threat posture**

Displays the threat posture of assets for the previous day. You can view how many DDoS, network, application, and server attacks detected, DDoS, WAF, and HSS inspection statistics, and network and server attack changes for the previous day. You can also view top 5 network, application, and server attack types, as well as the distribution of top 5 application attack sources, top 5 attacked applications, top 5 network attack sources, and the five servers with the most alerts.

- **Log analysis**

Displays the log statistics for **the previous day**, including log sources, log indexes, received logs, and log storage capacity as well as top 10 models that report the most alerts. It also displays logs analysis for **the past 7 days**, including log change trend and 5 log sources with the largest traffic volume.

- **Security Response**

Displays the security response information for **the previous day**, including the number of handled alerts, incidents, vulnerabilities, and risky baseline settings, distribution and quantity of threat alerts, distribution and quantity of top 5 intrusion incidents, top 5 emergency responses, and handling status of top 20 threat alerts.

- **External security hotspot**

Displays information about external security hotspots for **the previous day**.

7.3.3 Downloading a Report

You can download historical reports in PDF or .jpg to a local PC.

Procedure


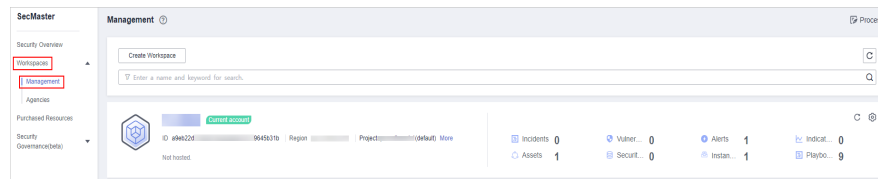
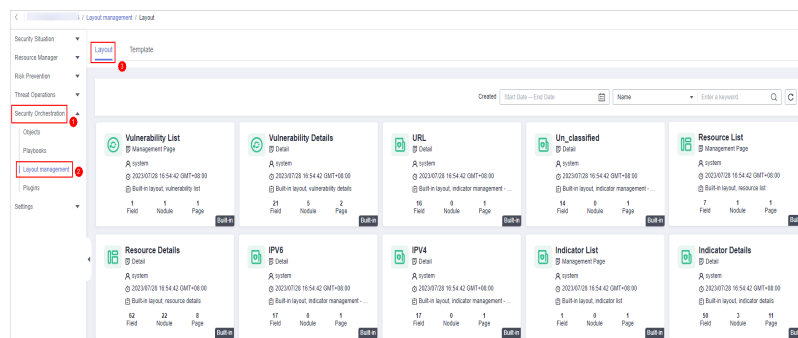
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.


Figure 7-15 Management



- Step 4** In the navigation tree on the left, choose **Security Orchestration > Layouts**. The **Layout** tab is displayed by default.

Figure 7-16 Layouts page



- Step 5** On the layout management page, move the mouse pointer to the daily report layout and click  in the upper right corner of the layout.
- Step 6** On the layout editing page, click the download button.


The system automatically downloads the security report in .jpg format to the local PC.

----End

7.3.4 Managing Security Reports

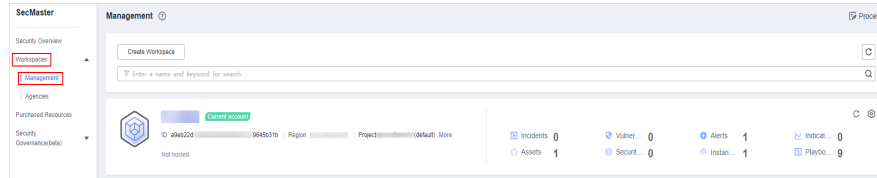
This section describes how to manage security reports, including enabling, disabling, editing, and deleting security reports.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.

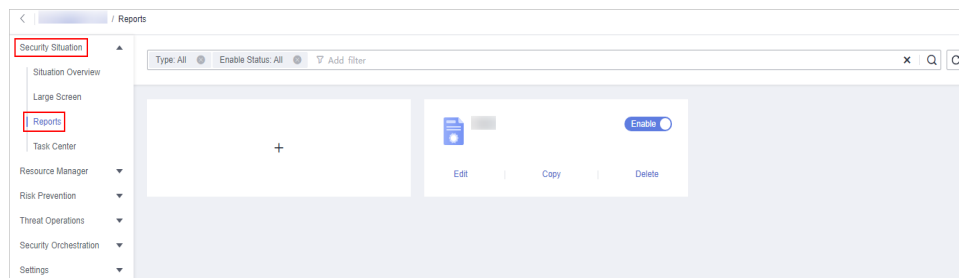
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-17 Management



Step 4 In the navigation pane on the left, choose **Security Situation > Reports**.

Figure 7-18 Reports



Step 5 Manage security reports.

Table 7-5 Managing security reports

Operation	Step
Enabling/disabling a security report	<p>On the Reports page, locate the desired report and toggle the slider on or off.</p> <ul style="list-style-type: none"> • If the slider is toggled on, the security report is enabled. • If the slider is toggled off, the security report is disabled.
Editing a Security Report	<ol style="list-style-type: none"> 1. On the Reports page, locate the desired report and click Edit. 2. (Optional) Edit basic report information. 3. Click Next: Report Choose. The Report Selection page is displayed. 4. (Optional) Select the report layout. 5. Click Complete in the lower right corner.
Deleting a Security Report	<ol style="list-style-type: none"> 1. On the Reports page, locate the desired report and click Delete. 2. In the Warning dialog box displayed, click OK.

----End

7.4 Task Center

7.4.1 Viewing To-Do Tasks

The to-do list displays the tasks that you need to process. This section describes how to view the to-do list.

Procedure


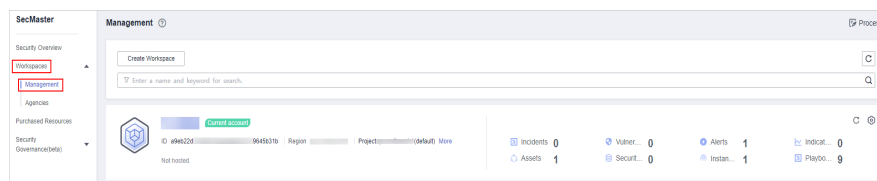
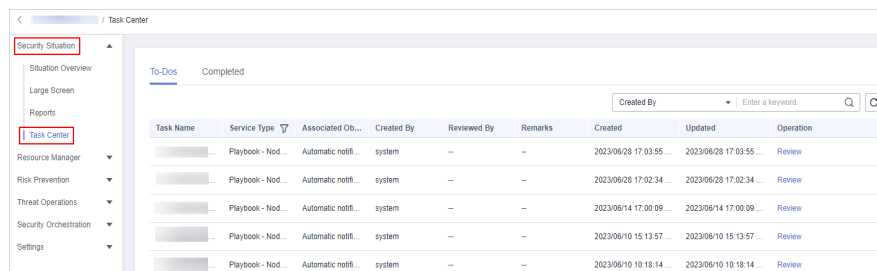
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-19 Management



- Step 4** In the navigation pane on the left, choose **Security Situation > Task Center**.

Figure 7-20 To-Dos



- Step 5** On the **To-Dos** tab page displayed, view details about the to-do tasks.


When there are a large number of to-do tasks, you can select **Created By** or **Task Name**, enter a keyword in the search box, and click  to quickly find the one you want.

Table 7-6 To-do task parameters

Parameter	Description
Task Name	Name of a task.

Parameter	Description
Service Type	Type of a task. <ul style="list-style-type: none"> • Workflow release • Playbook release • Playbook - Node Review
Associated Object	Name of the corresponding playbook or process.
Created By	Indicates the user who creates a task.
Reviewed By	Reviewer of the playbook/process
Created	Time when the playbook or process is created.
Updated	Last update time of the playbook or process.
Operation	Approve the to-do task.

----End

7.4.2 Handling a To-Do Task

When a playbook or process task reaches a node, the task needs to be suspended manually so that the playbook or process task can continue.

Process to-do tasks.

Prerequisites

A playbook task has been triggered, and manual actions are required for completing the task.

Procedure


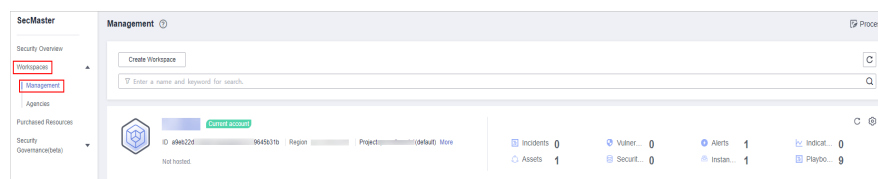
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 7-21 Management



- Step 4** In the navigation pane on the left, choose **Security Situation > Task Center**.

Figure 7-22 To-Dos

Task Name	Service Type	Associated Ob...	Created By	Reviewed By	Remarks	Created	Updated	Operation
	Playbook - Nod...	Automatic notifi...	system	--	--	2023/06/28 17:03:55 ...	2023/06/28 17:03:55 ...	Review
	Playbook - Nod...	Automatic notifi...	system	--	--	2023/06/28 17:02:34 ...	2023/06/28 17:02:34 ...	Review
	Playbook - Nod...	Automatic notifi...	system	--	--	2023/06/14 17:00:09 ...	2023/06/14 17:00:09 ...	Review
	Playbook - Nod...	Automatic notifi...	system	--	--	2023/06/10 15:13:57 ...	2023/06/10 15:13:57 ...	Review
	Playbook - Nod...	Automatic notifi...	system	--	--	2023/06/10 10:18:14 ...	2023/06/10 10:18:14 ...	Review

Step 5 In the row containing the target to-do task, click **Approve** in the **Operation** column.

The approval mode varies according to the service type.

- Playbook release: The **Playbook Release** page is displayed on the right. Enter review comments and approve the playbook as prompted.
- Process release: The **Process Release** page is displayed on the right. Enter the **Comment** and approve the application as prompted.
- Playbook-Node Review: The **Playbook-Node Review** page is displayed on the right. You can select **Continue** or **Terminate**.

----End

8 Resource Manager

8.1 Resource Manager Overview

SecMaster automatically discovers and manages all assets on and off the cloud and displays the real-time security status of your assets.

On the **Resource Manager** page, you can view the security status statistics of all resources under your account, including the resource name, service, and security status. This helps you quickly locate security risks and find solutions.

Asset Source and Corresponding Security Products

Table 8-1 Asset source and corresponding security products

Parameter	Source	Security Product
Servers	Elastic Cloud Server (ECS)	Host Security Service (HSS)
Website	Web Application Firewall (WAF)	Web Application Firewall (WAF)
Database	Relational Database Service (RDS)	Database Security Service (DBSS)
VPC	Virtual Private Cloud (VPC)	Cloud Firewall (CFW)
EIP	Elastic IP (EIP)	CNAD Basic (Anti-DDoS)
Device	On-premises devices	--

Note:

If the protection status of an asset on the SecMaster console is **Unprotected**, the corresponding security product is not enabled. If the protection status is -, the corresponding security product cannot be used in the region where the asset locates.

8.2 Modifying the Asset Information Synchronization Policy

For newly created workspaces, the asset synchronization policy is **automatically enabled**, and asset information is automatically synchronized to SecMaster once an hour by default.

Perform the operations in this section if you need to set the asset information synchronization policy.

Procedure


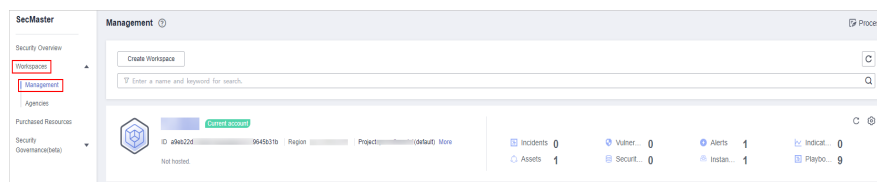
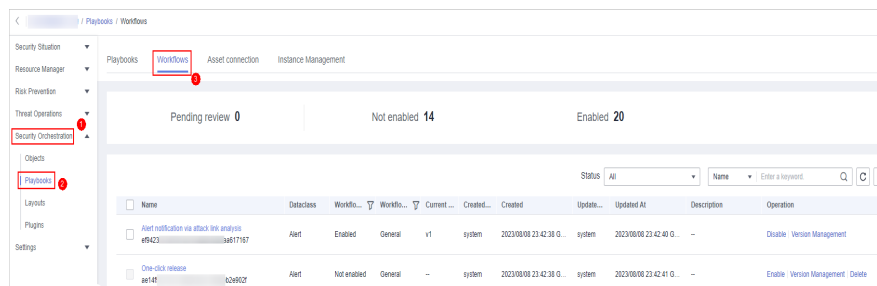
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 8-1 Management



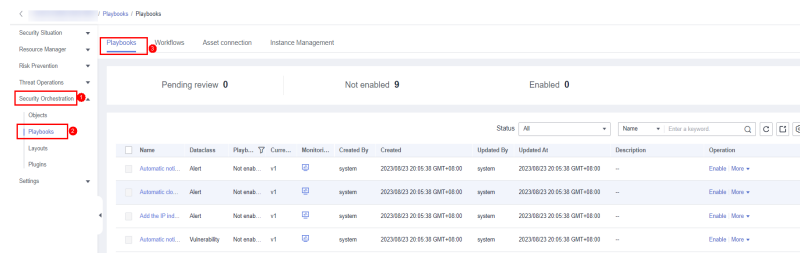
- Step 4** In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 8-2 Workflows tab page



- Step 5** In each row containing **RDS asset connection**, **VPC asset connection**, **Website asset connection**, **ECS asset connection**, or **EIP asset connection**, click **Enable** in the **Operation** column, respectively, to enable the workflows.
- Step 6** In the left navigation pane, choose **Security Orchestration > Playbooks**.

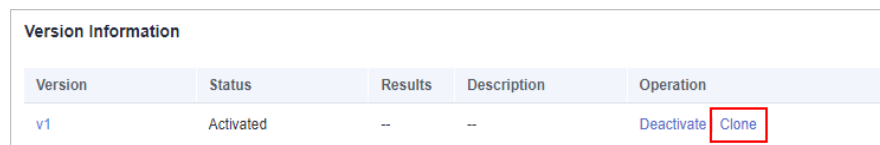
Figure 8-3 Accessing the Playbooks tab



Step 7 Add a playbook version.

1. Locate the row that contains the asset connection playbook, and click **Version Management** in the **Operation** column. The **Version Management** page is displayed.
2. In the **Version Information** area of the **Version Management** dialog box, locate the row of version **v1**, and click **Clone** in the **Operation** column. In the dialog box that is displayed, click **OK**.

Figure 8-4 Cloning a version



3. In the row that contains the draft version, click **Edit** in the **Operation** column. The editing pane is displayed on the right.
4. In the version information area on the editing pane, click **Add Condition** next to the trigger condition. The **Trigger Condition** page is displayed.

Figure 8-5 Adding a condition



5. On the **Trigger Condition** page, set the asset synchronization time.

Table 8-2 Parameters for configuring trigger conditions

Parameter	Description
Started	<ul style="list-style-type: none"> – Immediate: The playbook takes effect immediately after being created. – Custom: You can specify a time when the playbook can be triggered.

Parameter	Description
Execution Frequency	<ul style="list-style-type: none"> - Once: The task is executed only once within the time range. The task ends when the execution is complete. - Repeat: Set the repeated execution policy. Set the execution time to once every xx minutes, hours, days, or weeks. - Scheduled execution: The task is executed at the specified time. Set the execution time to xx hour xx minute xx second every day or every week.
End Conditions	<p>This parameter is mandatory when Execution Frequency is set to Repeat or Scheduled.</p> <ul style="list-style-type: none"> - Always Execute: The task does not have an end time. After the task is created, the task is executed at the specified time. - Custom: You can specify a time when the playbook ends.

6. Click **OK**.
7. After confirming that the information is correct, click **OK** in the lower right corner of the page.

Step 8 Submit the script version.

Locate the row of the **ECS Asset Connector** playbook and click **Submit** in the **Operation** column. In the dialog box that is displayed, click **OK**.

Step 9 Review the playbook version.

On the **Version Management** page, locate the row of the **ECS Asset Connector** playbook version and click **Review** in the **Operation** column. On the displayed **Review** page, click **OK** in the lower right corner of the page.

Step 10 Enable the playbook.

Locate the row of the **ECS Asset Connector** playbook and click **Enable** in the **Operation** column. In the dialog box that is displayed, click **OK**.

The system synchronizes data based on the latest enabled synchronization policy.


----End

8.3 Viewing Resource Information

On the **Resource Manager** page, you can view the name, type, and protection status of resources you have.

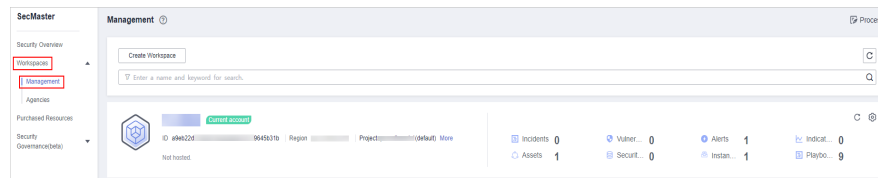
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

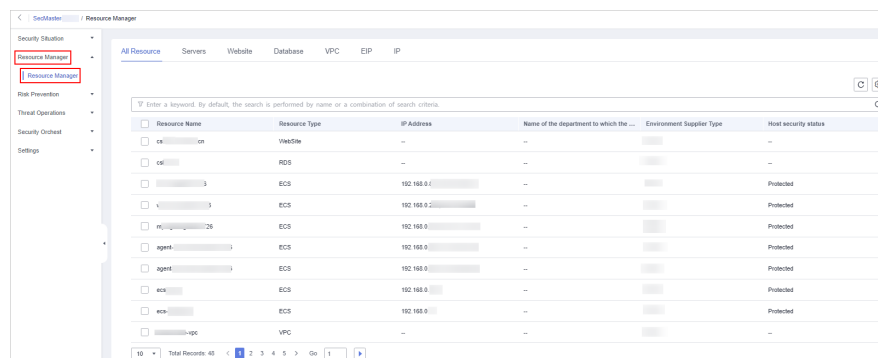
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 8-6 Management



Step 4 In the navigation pane on the left, choose **Resource Manager > Resource Manager**.

Figure 8-7 Resource Manager



Step 5 View resource details.

You can view details on **All Resource**, **Servers**, **Website**, **Database**, **VPC**, **EIP**, and **IP** tabs.

- All Resources

View the security status of all resources. **Table 8-3** describes related parameters.


If there are a large number of resources on this page, you can select **Resource Type** and enter a keyword in the search box, and click  to search for a specific resource.

Table 8-3 Parameters

Parameter	Description
Resource Name	Resource name
Resource Type	Type of the resource. For example, cloud servers, disks, and instances.
IP Address	IP address of a resource
Department	Name of the department to which a resource belongs

Parameter	Description
Environment Supplier Type	Type of the environment vendor of a resource
Host Security Status	Whether HSS is enabled for a resource

- Servers tab
You can view server information.

Table 8-4 Server information parameters

Parameter	Description
Resource Name	Name of a host
Image Name	Name of a host image
IP Address	IP address of a host
Department	Name of the department to which a host belongs
Environment Supplier Type	Type of the environment vendor of a host
Host Security Status	Whether HSS is enabled for a host
Description	Host description

- Website tab
You can view website information.

Table 8-5 Website parameters

Parameter	Description
Resource Name	Name of a website
DNS server list	Servers to which the domain name belongs
Department	Name of the department to which a website belongs
Environment Supplier Type	Type of the environment vendor of a website
WAF enabling status	Whether WAF is enabled for the domain name

- Database tab
You can view database information.

Table 8-6 Database parameters

Parameter	Description
Resource Name	Name of a database
Database Engine	Database engine type
External IP Address	External IP address of a database
Department	Name of the department to which a database belongs
Environment Supplier Type	Type of the environment vendor of a database
On state	Whether to database protection is enabled
Description	Description of the database

- VPC
You can view VPC information.

Table 8-7 VPC parameters

Parameter	Description
Resource Name	VPC name
Resource Type	VPC type
Subnet Scope	Range of a VPC subnet
Department	Department to which a VPC belongs
Environment Supplier Type	Type of the environment vendor of a VPC
Protection Status	Whether protection is enabled for a VPC
Description	Description about the VPC

- EIP tab
You can view EIP information.

Table 8-8 EIP parameters

Parameter	Description
Resource Name	EIP name
Public IP Address	Public IP address of the EIP
Department	Name of the department to which an EIP belongs

Parameter	Description
Environment Supplier Type	Type of the environment vendor of an EIP
Status	EIP status
Description	Description about the EIP

- IP tab
You can view IP address information.

Table 8-9 IP address parameters

Parameter	Description
Resource Name	Name of an IP address
Resource Type	Type of an IP address
Asset Value	Asset value of an IP address
Department	Name of the department to which an IP address belongs
Environment Supplier Type	Type of the environment vendor of an IP address
Asset Remarks	Remarks of the IP address

----End

8.4 Importing and Exporting Assets

SecMaster allows you to import assets outside the cloud. After the import, the security status of the assets can be displayed. You can also export asset information.


This section describes how to import and export assets.

Limitations and Constraints

Only .xlsx files no larger than 20 MB can be imported.

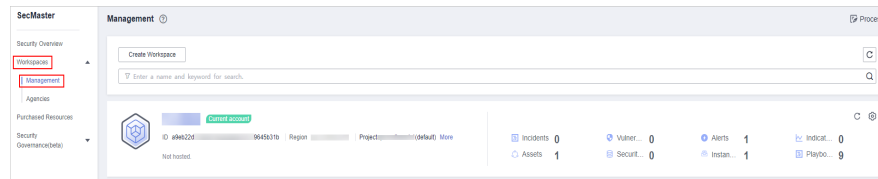
Importing Assets

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

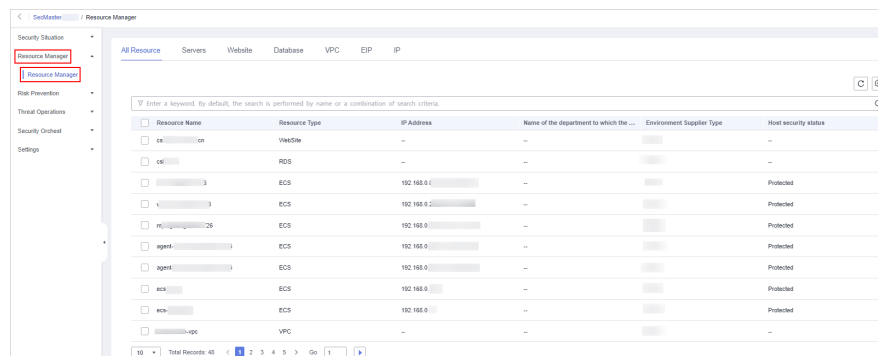
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 8-8 Management



Step 4 In the navigation pane on the left, choose **Resource Manager > Resource Manager**.

Figure 8-9 Resource Manager



Step 5 On the **Resource Manager** page, click a tab corresponding to the type of the resources you want to import.

Step 6 In the upper left corner of the asset list, click **Import**.

Step 7 In the **Import** dialog box, click **Download Template**. Then, fill information about the resource to be imported in the template.

CAUTION

- For details about how to enter the information, see [Asset Import Template Parameters](#).
- The file must be in the .xlsx format.

Step 8 After the template is filled, click **Select File** in the **Import** dialog box and select the Excel file you want to import.

Step 9 Click **OK**.

----End

Asset Import Template Parameters

You can use a template to import assets in batches. For details about the parameters in the asset import template, view the following tables:

- [Servers](#)
- [Websites](#)
- [Databases](#)

- [VPC](#)
- [EIP](#)
- [IP addresses](#)

 **NOTE**

Do not modify the table heads when you use the template.

Table 8-10 Servers

Parameter	Type	Mandatory	Description
id	String	Yes	Asset ID, which contains 2 to 36 characters.
name	String	Yes	Asset name, which contains 2 to 512 characters.
protected_statuses	String	No	Whether HSS is enabled <ul style="list-style-type: none"> • OPEN: HSS is enabled. • CLOSE: HSS is disabled.
description	String	No	ECS description
status	String	No	ECS status The value can be any of the following: ACTIVE, BUILD, ERROR, HARD_REBOOT, MIGRATING, REBOOT, REBUILD, RESIZE, REVERT_RESIZE, SHUTOFF, VERIFY_RESIZE, DELETED.
host_id	String	No	ID of the server where the ECS is deployed.
host_name	String	No	Name of the server where the ECS is deployed.
host_status	String	No	Status of the server where the ECS is deployed. The value can be any of the following: <ul style="list-style-type: none"> • UP: The server is running properly. • UNKNOWN: The server status is unknown. • DOWN: The server is abnormal. • MAINTENANCE: The server is under maintenance. • Null: The ECS does not have host information.

Parameter	Type	Mandatory	Description
version	String	No	IP address version <ul style="list-style-type: none"> • 4: IPv4 • 6: IPv6
addr	String	No	IP address
type	String	No	IP address type fixed : private IP address floating : floating IP address
mac_addr	String	No	MAC address
port_id	String	No	ID of the port bound to the IP address
vpc_id	String	No	ID of the VPC to which the ECS belongs
image_type	String	No	Image class. The following classes are supported: <ul style="list-style-type: none"> • gold: Public image • private: Private image • shared: Shared image
image_name	String	No	Image name of the ECS
os_type	String	No	OS type. The value can be Linux or Windows .
os_bit	String	No	OS architecture, 32 bit or 64 bit.
resource_spec_code	String	No	Resource specifications of the ECS
vendor_type	String	Yes	Environment supplier
domain_id	String	Yes	ID of the tenant to which the asset belongs.
region_id	String	Yes	Asset region.
project_id	String	Yes	ID of the project to which the asset belongs.
ep_id	String	No	ID of the enterprise project to which the asset belongs.
ep_name	String	No	Name of the enterprise project to which the asset belongs.
vendor_name	String	Yes	Asset probes or asset providers

Parameter	Type	Mandatory	Description
idc_id	String	Yes	ID of the on-premises equipment room
idc_name	String	Yes	Name of the on-premises equipment room
department_name	String	No	Name of the department to which the asset belongs
business_name	String	No	Name of the service system
business_owner	String	No	Owner of the service system
governance_user_type	String	No	Type of the asset governance owner
governance_user_name	String	No	Name of the asset governance owner

Table 8-11 Websites

Parameter	Type	Mandatory	Description
value	String	Yes	Website name
domain_name	String	Yes	Domain name
name_server	String	No	DNS servers. Use commas (,) to separate IP addresses, for example, 192.168.25.106,192.168.25.124 .
protected_statuses	String	No	Whether WAF is enabled. <ul style="list-style-type: none"> OPEN: WAF is enabled. CLOSE: WAF is disabled. If this parameter left blank, the default value CLOSE will be used.
idc_id	String	Yes	ID of the on-premises data center
idc_name	String	Yes	Name of the on-premises data center
vendor_name	String	Yes	Asset provider
department_name	String	No	Name of the department to which the asset belongs
business_name	String	No	Name of the service system

Parameter	Type	Mandatory	Description
business_owner	String	No	Owner of the service system
governance_user_type	String	No	Type of the asset governance owner
governance_user_name	String	No	Name of the asset governance owner

Table 8-12 Databases

Parameter	Type	Mandatory	Description
id	String	Yes	Instance ID
name	String	Yes	Instance name

Parameter	Type	Mandatory	Description
status	String	Yes	<p>Instance status. The value can be any of the following:</p> <ul style="list-style-type: none"> ● BUILD: The instance is being created. ● ACTIVE: The instance is running properly. ● FAILED: The instance is abnormal. ● FROZEN: The instance is frozen. ● MODIFYING: The instance is being scaled up. ● REBOOTING: The instance is being restarted. ● RESTORING: The instance is being restored. ● MODIFYING INSTANCE TYPE: The instance is changing to the active/standby deployment. ● SWITCHOVER: The instance is performing an active/standby switchover. ● MIGRATING: The instance is being migrated. ● BACKING UP: The instance is being backed up. ● MODIFYING DATABASE PORT: The database port of the instance is being changed. ● STORAGE FULL: The instance disk is full.
private_ips	String	Yes	<p>Private IP addresses. Use commas (,) to separate IP addresses, for example, 192.168.25.106,192.168.25.124.</p>

Parameter	Type	Mandatory	Description
port	Integer	Yes	<p>Database port number</p> <ul style="list-style-type: none"> An RDS for MySQL database can use ports 1024 to 65535, excluding 12017 and 33071, which are reserved for RDS system use. An RDS for PostgreSQL database can use ports 2100 to 9500. An RDS for SQL Server DB instance port is 1433 or any value from 2100 to 9500 (excluding 5355 and 5985). For Microsoft SQL Server 2017 Enterprise, Standard, and Web editions, the database port cannot be 5050, 5353, or 5986.
enable_ssl	Boolean	Yes	<p>Whether SSL is enabled</p> <ul style="list-style-type: none"> true: SSL is enabled for the instance. false: SSL is disabled for the instance.
type	String	Yes	<p>Instance type. The value can be any of the following:</p> <ul style="list-style-type: none"> Single: single-node instance Ha: Instance in active/standby deployment Replica: read replica instance Enterprise: distributed instance (enterprise edition)
region	String	Yes	Region to which the asset belongs
db_user_name	String	Yes	Default username
vpc_id	String	Yes	VPC ID
subnet_id	String	Yes	Network ID of the subnet
cpu	String	Yes	Number of CPUs.
mem	String	Yes	Memory size in GB
vendor_type	String	Yes	Environment supplier
domain_id	String	Yes	ID of the tenant to which the asset belongs.
region_id	String	Yes	Asset region.

Parameter	Type	Mandatory	Description
project_id	String	Yes	ID of the project to which the asset belongs.
ep_id	String	No	ID of the enterprise project to which the asset belongs.
ep_name	String	No	Name of the enterprise project to which the asset belongs.
vendor_name	String	Yes	Asset probes or asset providers
idc_id	String	Yes	ID of the on-premises equipment room
idc_name	String	Yes	Name of the on-premises equipment room
department_name	String	No	Name of the department to which the asset belongs
business_name	String	No	Name of the service system
business_owner	String	No	Owner of the service system
governance_user_type	String	No	Type of the asset governance owner
governance_user_name	String	No	Name of the asset governance owner

Table 8-13 VPC

Parameter	Type	Mandatory	Description
id	String	Yes	VPC ID
name	String	Yes	VPC name
protected_statuses	String	No	Security status. The value can be OPEN (protection enabled) or CLOSE (protection disabled).
description	String	No	Description about the VPC
cidr	String	Yes	Range of available subnets in the VPC

Parameter	Type	Mandatory	Description
status	String	Yes	VPC status. The options are as follows: <ul style="list-style-type: none"> ● PENDING: The VPC is being created. ● ACTIVE: The VPC is created.
vendor_type	String	Yes	Provider type
domain_id	String	Yes	ID of the tenant to which the asset belongs.
region_id	String	Yes	ID of the asset region.
project_id	String	Yes	ID of the project to which the asset belongs.
ep_id	String	No	ID of the enterprise project to which the asset belongs.
ep_name	String	No	Name of the enterprise project to which the asset belongs.
vendor_name	String	Yes	Asset probes or asset providers
idc_id	String	Yes	ID of the on-premises equipment room
idc_name	String	Yes	Name of the on-premises equipment room
department_name	String	No	Name of the department to which the asset belongs
business_name	String	No	Name of the service system
business_owner	String	No	Owner of the service system
governance_user_type	String	No	Type of the asset governance owner
governance_user_name	String	No	Name of the asset governance owner

Table 8-14 EIP

Parameter	Type	Mandatory	Description
id	String	Yes	Unique ID
alias	String	No	EIP Name

Parameter	Type	Mandatory	Description
description	String	No	Description about the EIP
protected_statuses	String	No	Anti-DDoS or CFW status. The value can be OPEN (the function is enabled) or CLOSE (the function is disabled).
project_id	String	Yes	Project ID
ip_version	Integer	Yes	IP address version The options are as follows: <ul style="list-style-type: none"> • 4 • 6
public_ip_addresses	String	Yes	IP Address
publicip_pool_name	String	Yes	Network type of an EIP, including public EIP pool (for example, 5_bgp or 5_sbgp) and dedicated EIP pool.
status	String	Yes	EIP status. The options are as follows: <ul style="list-style-type: none"> • FREEZED: The EIP is frozen. • BIND_ERROR: The EIP fails to be bound. • BINDING: The EIP is being bound. • PENDING_DELETE: The EIP is being released. • PENDING_CREATE: The EIP is being created. • NOTIFYING: The EIP is being created. • NOTIFY_DELETE: The EIP is being released. • PENDING_UPDATE: The EIP is being updated. • DOWN: The EIP has not been bound. • ACTIVE: The EIP has been bound. • ELB: The EIP has been bound to an ELB load balancer. • VPN: The EIP has been bound to a VPN. • ERROR: The EIP is failed.

Parameter	Type	Mandatory	Description
associate_instance_type	String	Yes	Type of the instance to which the EIP address is bound. The options are as follows: <ul style="list-style-type: none"> • PORT • NATGW • ELB • ELBV1 • VPN • null
associate_instance_id	String	Yes	ID of the instance to which the EIP address is bound
create_time	String	Yes	UTC time when a resource is created ISO8601 format: YYYY-MM-DDTHH:mm:ss.ms+timezone
vendor_type	String	Yes	Provider type
domain_id	String	Yes	ID of the tenant to which the asset belongs.
region_id	String	Yes	ID of the asset region.
project_id	String	Yes	ID of the project to which the asset belongs.
ep_id	String	No	ID of the enterprise project to which the asset belongs.
ep_name	String	No	Name of the enterprise project to which the asset belongs.
vendor_name	String	Yes	Asset probes or asset providers
idc_id	String	Yes	ID of the on-premises equipment room
idc_name	String	Yes	Name of the on-premises equipment room
department_name	String	No	Name of the department to which the asset belongs
business_name	String	No	Name of the service system
business_owner	String	No	Owner of the service system
governance_owner_type	String	No	Type of the asset governance owner

Parameter	Type	Mandatory	Description
governance_user_name	String	No	Name of the asset governance owner


Table 8-15 IP addresses

Parameter	Type	Mandatory	Description
value	String	Yes	Asset value
version	String	Yes	Asset Type <ul style="list-style-type: none"> • ipv4 • ipv6
relative_value	String	No	Opposite value. For example, if the IP address is an IPv4 address, the value is ipv6 .
network_public	Boolean	Yes	External network or internal network
network_partition	String	No	Network partition: OM/PSZ/DMZ
network_partition	String	No	Network plane code
network_vxlan_id	String	No	Virtual network ID
remark	String	No	Asset remarks
name	String	No	Asset name. The default value is the asset value.
latitude	Float	No	Latitude
longitude	Float	No	Longitude
city_code	String	Yes	City code. Set this parameter based on the standard city code.
country_code	String	Yes	Country code. Set this parameter based on the international standard country code.
server_room	String	Yes	Equipment room
server_rack	String	Yes	Cabinet
mac_addr	String	No	MAC address

Parameter	Type	Mandatory	Description
important	String	Yes	Severity <ul style="list-style-type: none"> • 0: minor • 1: major
idc_id	String	Yes	ID of the on-premises data center
idc_name	String	Yes	Name of the on-premises data center
vendor_name	String	Yes	Asset provider
department_name	String	No	Name of the department to which the asset belongs
business_name	String	No	Name of the service system
business_owner	String	No	Owner of the service system
governance_user_type	String	No	Type of the asset governance owner
governance_user_name	String	No	Name of the asset governance owner

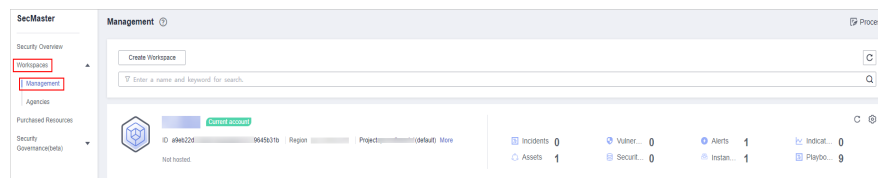
Exporting Assets

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

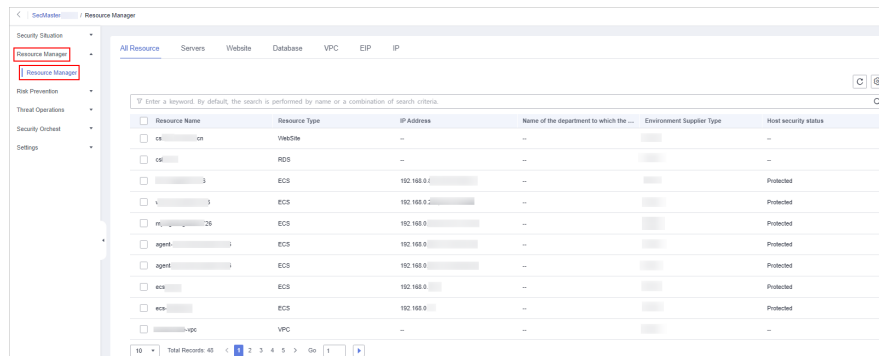
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 8-10 Management




Step 4 In the navigation pane on the left, choose **Resource Manager > Resource Manager**.

Figure 8-11 Resource Manager



Step 5 On the asset management page, click the corresponding asset tab.

Step 6 On the asset page, select the assets to be exported and click  in the upper right corner of the list.

Step 7 In the **Export** dialog box, set asset parameters.

Table 8-16 Exporting assets

Parameter	Description
Format	By default, the asset list is exported into an Excel.
Columns	Select the parameters to be exported.

Step 8 Click **OK**.

The system automatically downloads the Excel to your local PC.

----End

8.5 Deleting an Asset


You can delete cloud assets or assets you imported into SecMaster on the resource manager page.

Limitations and Constraints

Only assets imported outside the cloud can be deleted.

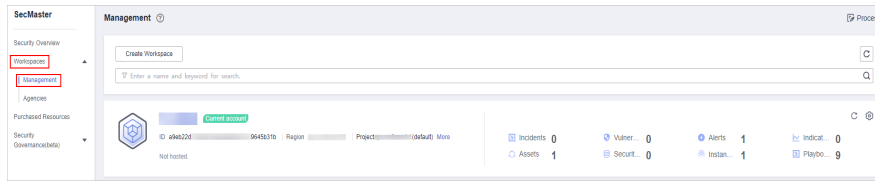
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

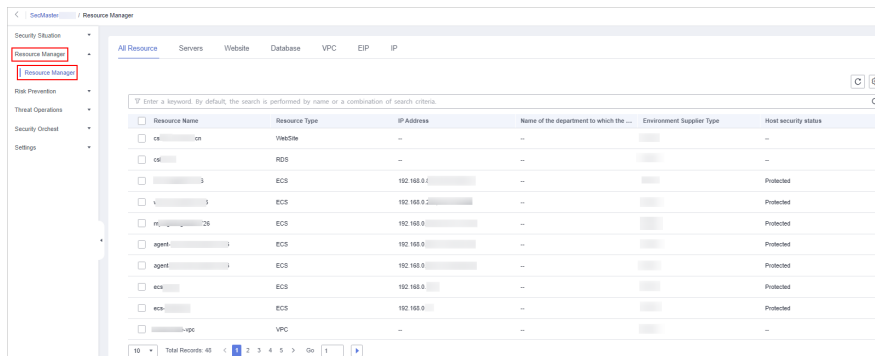
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 8-12 Management



Step 4 In the navigation pane on the left, choose **Resource Manager > Resource Manager**.

Figure 8-13 Resource Manager



Step 5 On the asset management page, click the corresponding asset label. The asset page is displayed.

Step 6 On the asset page, select the assets to be deleted and click **Batch Delete** above the list.

The system will delete the selected assets.

----End

9 Risk Prevention

9.1 Baseline Inspection

9.1.1 Cloud Service Baseline Overview

SecMaster can check cloud service baseline settings. It can scan cloud services for risks in key configuration items, report scan results by category, generate alerts for incidents, and provide hardening suggestions and guidelines.

9.1.2 Configuring a Baseline Inspection Plan

You can configure a baseline inspection plan and let SecMaster check whether there are unsafe baseline configurations on your servers.

This document describes how to add, edit, and delete a baseline inspection plan.

Background

After you enable baseline inspection, SecMaster will check all of your assets based on the default check plan. By default, the default check plan works as follows:


- **Schedule:** The default check plan checks your assets every three days from 00:00 to 06:00.
- **Objects:** All assets under your account in the current region will be checked.

Limitations and Constraints

A security standard can be added to only one check plan.

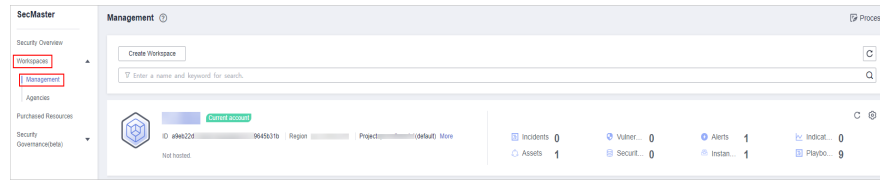
Creating a Check Plan

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

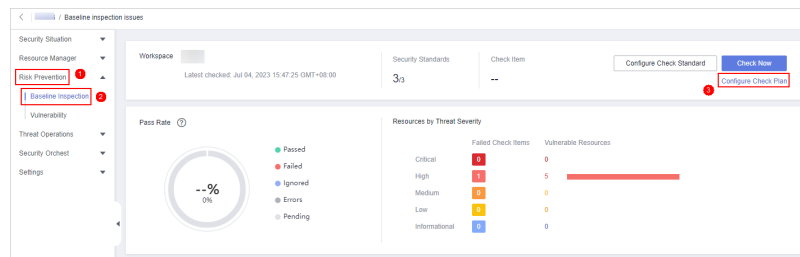
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-1 Management



Step 4 In the navigation tree on the left, choose **Risk Prevention > Baseline Inspection**. On the **Baseline Inspection** page, click **Configure Check Plan**.

Figure 9-2 Accessing the page for configuring check plans



Step 5 On the **Checks** page, select a region for the plan and click **Create Plan**. The pane for creating a check plan is displayed on the right.

Step 6 Configure the check plan.

1. Enter the basic information by referring to [Table 9-1](#).

Table 9-1 Basic information about a check plan

Parameter	Description
Name	Plan name
Schedule	Select how often and when the check plan is executed. <ul style="list-style-type: none"> - Schedule: every day, every 3 days, every 7 days, every 15 days, or every 30 days - Check start time: 00:00-06:00, 06:00-12:00, 12:00-18:00, or 18:00-24:00

2. Select a security standard for the plan.
Select the baseline check items to be checked.

Step 7 Click **OK**.

After the check plan is created, SecMaster performs cloud service baseline scanning at the specified time. You can choose **Risk Prevention > Baseline Inspection** to view the scan result.

----End

Related Operations

After a baseline check plan is created, you can view, edit, or delete the check plan.

- Viewing a check plan
 - a. In the navigation pane on the left, choose **Settings > Checks**.
 - b. On the **Checks** page, view the check plans of baseline inspection.
- Editing a check plan

Only user-defined check plans can be modified.

 - a. In the navigation pane on the left, choose **Settings > Checks**.
 - b. In the upper right corner of the check plan box, click **Edit**. The pane for editing the check plan is displayed on the right.
 - c. After editing the plan parameters, click **OK**.
- Deleting a check plan

Only user-defined check plans can be deleted.

 - a. In the navigation pane on the left, choose **Settings > Checks**.
 - b. In the upper right corner of the check plan box, click **Delete**.
 - c. In the displayed dialog box, click **OK**.

9.1.3 Executing a Baseline Inspection Plan

To learn about the latest status of the cloud service baseline configurations, execute or let SecMaster execute a check plan. Then you can view which configurations are unsafe in the check results.

The baseline inspection supports periodic and immediate checks.


- Periodic check: SecMaster periodically executes the default check plan or the check plans you configure. SecMaster executes the default check plan at 00:00 every three days.
- Immediate check: You can add or modify a custom check plan and start the check plan immediately. In this way, you can check whether the servers have certain unsafe configurations in real time.

Limitations and Constraints

- An immediate check task can be executed only once within 10 minutes.
- A periodic check can be manually started only once within 10 minutes.

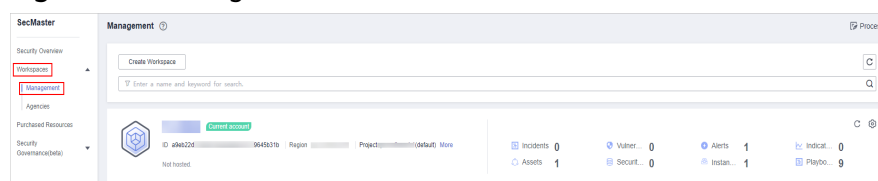
Starting a Check Based on Selected Standards

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

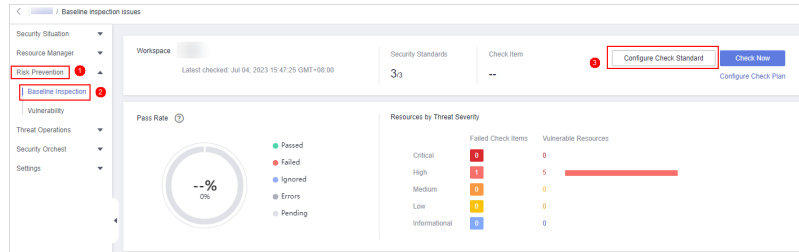
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-3 Management



Step 4 In the navigation pane on the left, choose **Baseline Inspection**. In the upper right corner of the page, click **Configure Check Standard**.

Figure 9-4 Baseline Inspection



Step 5 In the displayed **Select Security Standard** dialog box, select a standard and click **OK**.

Step 6 In the upper right corner of the page, click **Check Now**.


Refresh the page. To check whether the displayed result is the latest, click **View Details** in the **Operation** column and check the time in **Latest Check**.

----End

Starting a Check Based on a Check Plan

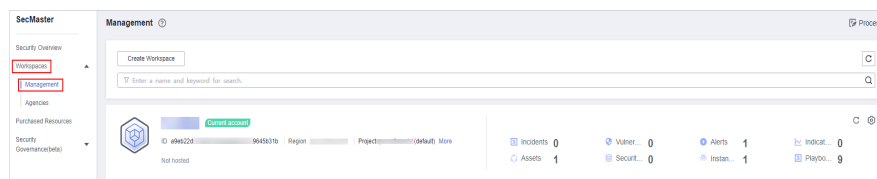
The following describes how to manually execute a check plan immediately.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

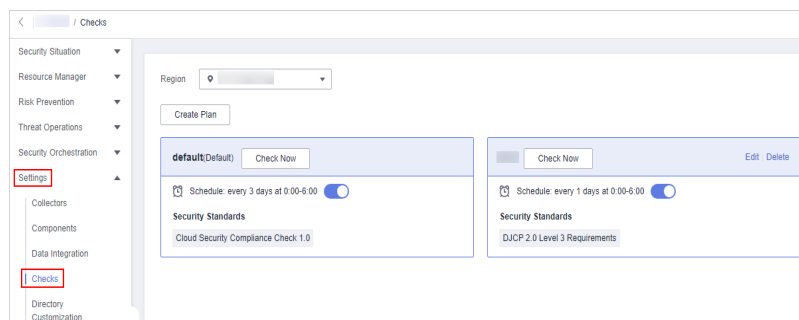
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-5 Management



Step 4 In the navigation pane on the left, choose **Settings > Checks**.

Figure 9-6 Checks page



Step 5 In a check plan box, click **Check Now**.

SecMaster immediately executes the selected baseline check plan.

----End

9.1.4 Handling Manual Check Items

Baseline check items are classified into automatic check items and manual check items. This section describes how to handle manual check items.


There are some manual check items included in baseline inspection. After you finish a manual check, report the check results to SecMaster. The pass rate is calculated based on results from both manual and automatic checks.

Constraints and Limitations

Manual check results must be reported every 7 days as your feedback is valid only for 7 days.

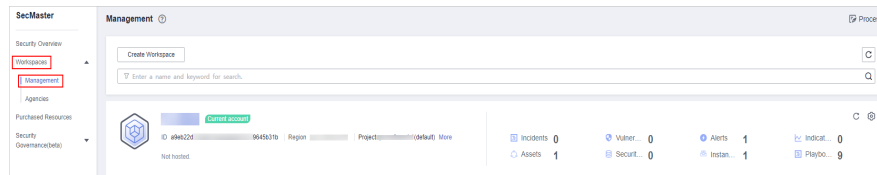
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

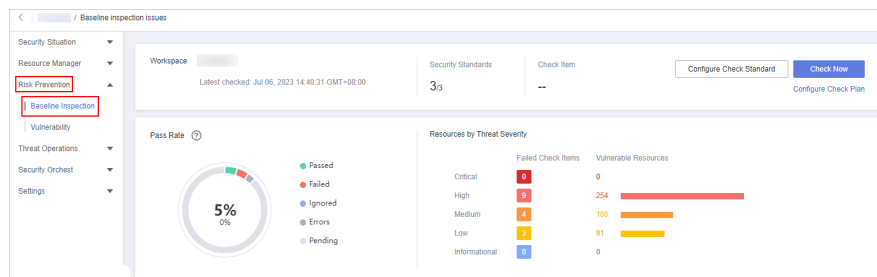
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-7 Management



Step 4 In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**.

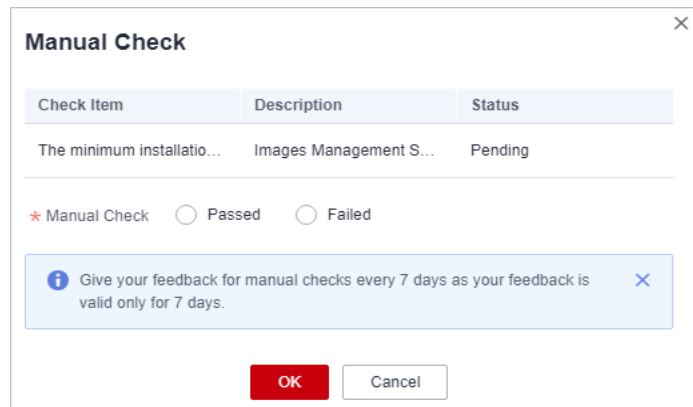
Figure 9-8 Accessing the baseline inspection page



Step 5 On the **Security Standards** tab page, locate the row that contains the check item whose result you need to report to SecMaster manually, click **Manual Check** in the **Operation** column.

Step 6 In the displayed dialog box, select a result and click **OK**.

Figure 9-9 Providing manual check results



NOTE

Report manual check results every 7 days as your feedback is valid only for 7 days.

----End

9.1.5 Viewing Baseline Inspection Results

You can learn about the affected assets and details about the baseline inspection items.

Procedure

View the check results of all check items in a region.


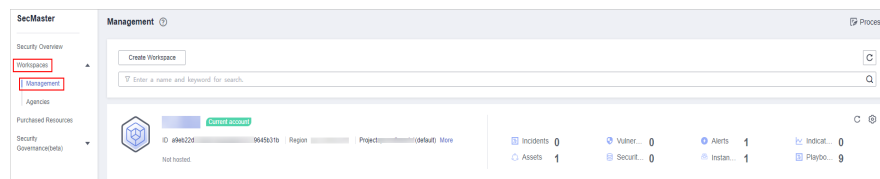
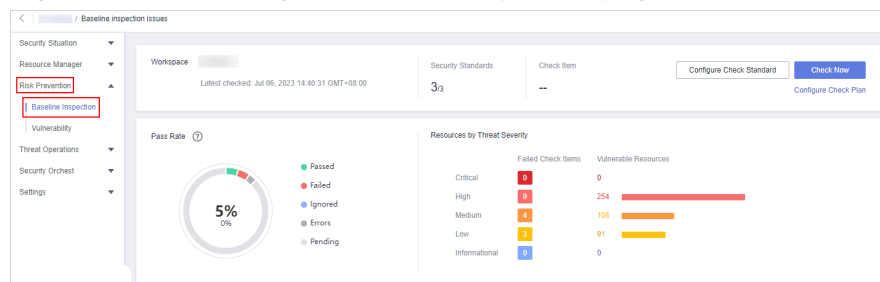
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-10 Management



- Step 4** In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**.

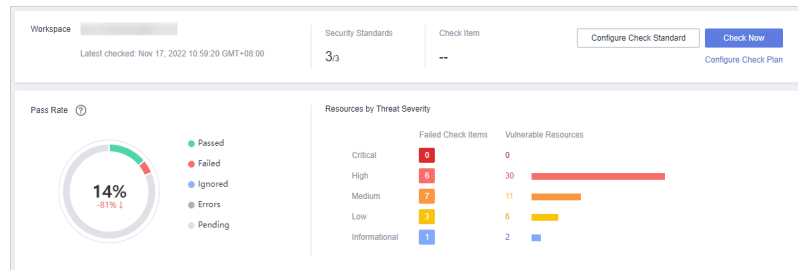
Figure 9-11 Accessing the baseline inspection page



Step 5 View overall check results.

On the **Baseline Inspection** page, view the baseline check result summary of the current workspace.

Figure 9-12 Check result statistics



- **Security Standards:** Number of security standards used for the latest check/ Total security standards
- **Check Item:** total number of check items in the latest baseline check
- **Pass Rate:** check item pass rate of the latest baseline check.
Overall pass rate = Passed check items/Total check items
The total check items are the sum of items in all the checked standards.
The check result can be **Passed, Failed, Errors, or Pending.**
- **Resources by Threat Severity:** displays the number of vulnerable resources by severity.
Severity: Critical, High, Medium, Low, and Informational.

Step 6 View the check result of all security standards.

1. Select **All**. The system displays all security standards and their details for the current region.
The **Security Standards** tab displays all baseline check standards and other details, including the check item, status, category, vulnerable resources, description, and latest check time.

NOTE

- You can select a baseline check standard and view the baseline check items included in the standard.
2. To view details about a baseline check item, click **View Details** in the **Operation** column.
On the **Baseline inspection issues** page, view the detailed description, check result, and suggestions of the check item.

Step 7 View the resource check result.

Only checked resources are listed.

1. Click the **Resources to Check** tab. All checked resources in the current region and their details are displayed.
The **Resources to Check** tab displays all checked resources and their details, including the resource name, resource type, check items, and vulnerable items.

Figure 9-13 All resources to check

NameID	Resource Type	Check Item	Vulnerable Item	Operation
image_	iam_user	1	1	Check View Details
Test_	iam_user	1	1	Check View Details
windows_	iam_user	1	1	Check View Details
image_	iam_user	1	1	Check View Details
DevCloud_	iam_user	1	1	Check View Details
OBS_	iam_user	1	1	Check View Details
DevCloud_	iam_user	1	1	Check View Details
OBS_	iam_user	1	1	Check View Details
DevCloud_	iam_user	1	1	Check View Details
HDN_	iam_user	1	1	Check View Details

- To view the check details of a resource, locate the row that contains the target resource and click **View Details** in the **Operation** column.
On the resource details page, view the check items, check status, check method, and last check time of the resource.

Step 8 View check results

Click the **Result** tab. All the check results in the current region and their details are displayed.

The **Result** tab lists all check results and their details, including the check items, check results, resource types, resource names, and latest check time.

Figure 9-14 All check results

Check Item	Result	Resource Type	Resource NameID	Schedule	Operation
IAM user login protection	Passed	iam_user	DevCloud_	Jul 04, 2023 15:47:20 GMT+08:00	Check View Details
IAM user login protection	Passed	iam_user	op_	Jul 04, 2023 15:47:24 GMT+08:00	Check View Details
IAM user login protection	Failed	iam_user	windows_	Jul 04, 2023 15:47:25 GMT+08:00	Check View Details
IAM user login protection	Passed	iam_user	OBS_	Jul 04, 2023 15:47:24 GMT+08:00	Check View Details
IAM user login protection	Failed	iam_user	image_	Jul 04, 2023 15:47:24 GMT+08:00	Check View Details
IAM user login protection	Passed	iam_user	VPC_	Jul 04, 2023 15:47:25 GMT+08:00	Check View Details
IAM user login protection	Failed	iam_user	Test_	Jul 04, 2023 15:47:25 GMT+08:00	Check View Details
IAM user login protection	Passed	iam_user	odk_	Jul 04, 2023 15:47:24 GMT+08:00	Check View Details
IAM user login protection	Failed	iam_user	image_	Jul 04, 2023 15:47:24 GMT+08:00	Check View Details
IAM user login protection	Passed	iam_user	OBS_	Jul 04, 2023 15:47:24 GMT+08:00	Check View Details

----End

9.1.6 Handling Baseline Inspection Results

To handle the check result, perform the following operations:

- Handling Unsafe Settings:** Rectify the risk check items based on the check result.
- Reporting Manual Check Results to SecMaster:** For manual check items, after you finish each check, report the check result to SecMaster. The pass rate is calculated based on results from both manual and automatic checks.
- Ignoring a Check Item:** If you have custom requirements for a check item, ignore the check item. For example, SecMaster checks whether the session timeout duration is set to 15 minutes, while you need to set it to 20 minutes.


In this situation, ignore this check item so that SecMaster no longer executes this check.

Prerequisites

- The cloud service baseline has been scanned.

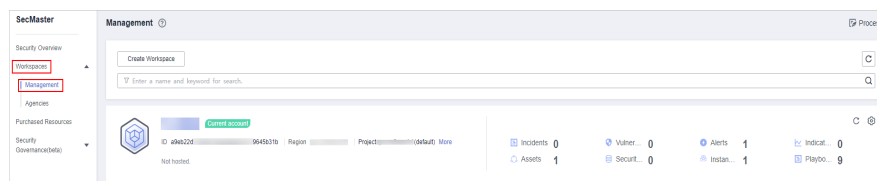
Handling Unsafe Settings

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

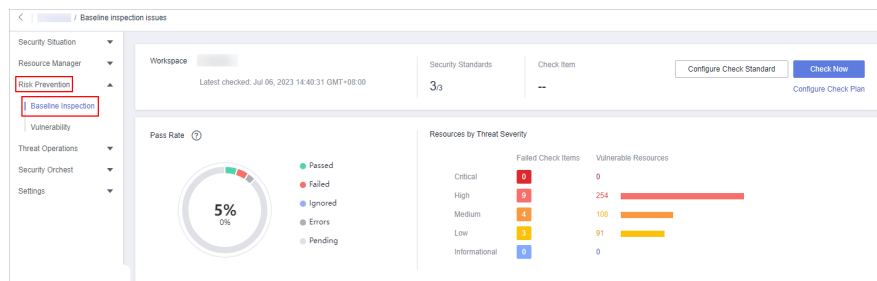
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-15 Management



Step 4 In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**.

Figure 9-16 Accessing the baseline inspection page



Step 5 On the **Security Standards** tab, select check items and view the risk status.

Step 6 Locate the row that contains the target sub-check item, click **View Details** in the **Operation** column. The check item details page is displayed.

Step 7 View the risk details and fix the unsafe settings by referring to **Result** and **Reference**.

Table 9-2 Check items

Parameter	Description
Status	<p>Displays the check status of the current check item.</p> <ul style="list-style-type: none"> If the result is Passed, the configuration corresponding to the check item is appropriate. If the result is Failed, the configuration corresponding to the check item is inappropriate. The check results will be listed.
Latest Check	Last time when the current check item was performed.
Check Method	Method used by the current check item.
Severity	Severity of the unsafe settings discovered against the current check item.
Impact	Security impact caused by unsafe settings discovered against the current check item.
Standard and Category	Security standard and category of the current check item.
Description	Check content of the current check items.
Check Process	Check process of the current check item.
Reference	<p>Links of documentation related to the check item.</p> <p>Click the reference link to go to the detailed page.</p>
Resource	<p>Resource to which the current check item belongs.</p> <p>The check result can be Passed or Failed.</p> <ul style="list-style-type: none"> If the result is Passed, the configuration corresponding to the check item is appropriate. If unsafe settings are found, the detailed information is listed. You can click the button in the Operation column to go to page and fix the configuration.


Step 8 After all unsafe configurations are rectified, click **Check** to verify that all risky items have been rectified.

----End

Reporting Manual Check Results to SecMaster

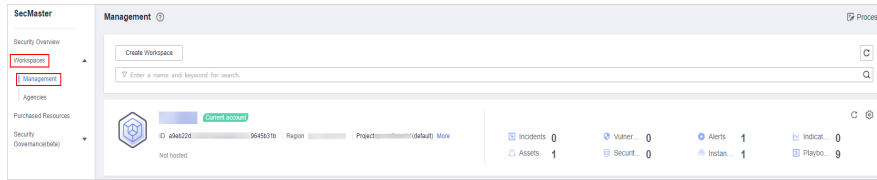
For manual check items, after you finish each check, report the check result to SecMaster. The pass rate is calculated based on results from both manual and automatic checks.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

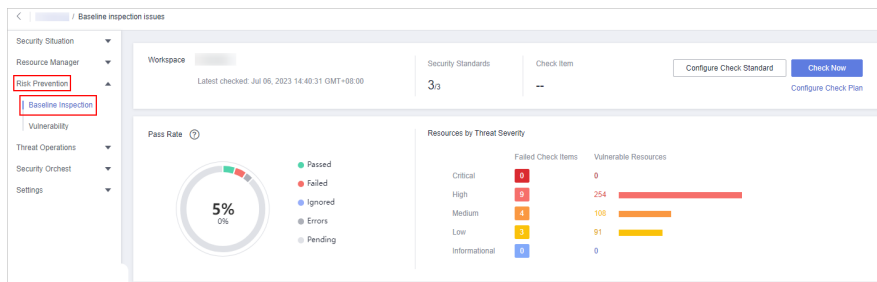
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-17 Management



Step 4 In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**.

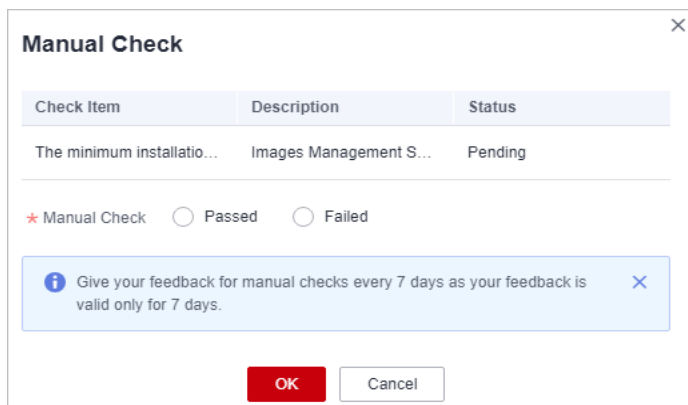
Figure 9-18 Accessing the baseline inspection page



Step 5 On the **Security Standards** tab page, locate the row that contains the check item whose result you need to report to SecMaster manually, click **Manual Check** in the **Operation** column.

Step 6 In the displayed dialog box, select a result and click **OK**.

Figure 9-19 Providing manual check results



NOTE

Report manual check results every 7 days as your feedback is valid only for 7 days.

----End


Ignoring a Check Item

If you have custom requirements for a check item, ignore the check item. For example, SecMaster checks whether the session timeout duration is set to 15

minutes, while you need to set it to 20 minutes. In this situation, ignore this check item so that SecMaster no longer executes this check.

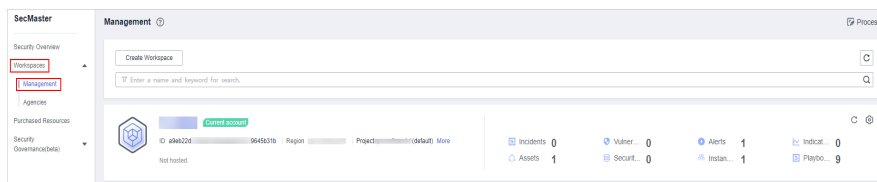
An ignored check item will be no longer executed. It will not be counted when the **Pass Rate** is calculated.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

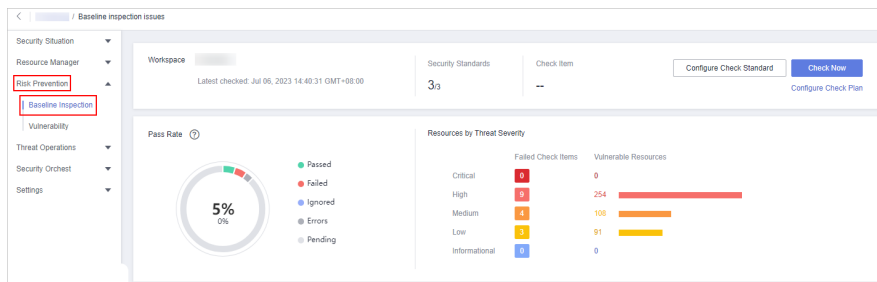
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-20 Management



Step 4 In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**.

Figure 9-21 Accessing the baseline inspection page

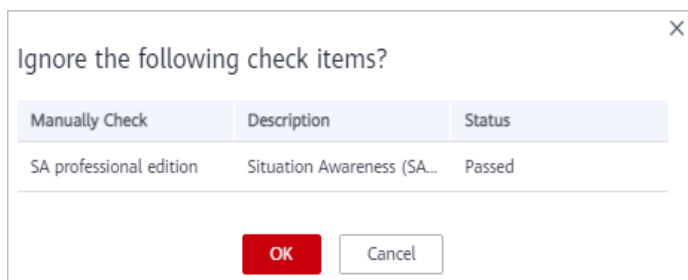


Step 5 On the **Security Standards** tab, locate the row containing the check item you want to ignore, click **Ignore** in the **Operation** column.

To ignore more than one check item at a time, select all the check items you want to ignore, and click **Ignore** in the upper left corner of the check item list.

Step 6 In the displayed dialog box, click **OK**.

Figure 9-22 Example confirming the ignore operation



 **NOTE**

- The ignored check items will be not executed. They will not be counted when the **Pass Rate** is calculated.
- To resume an ignored check item, locate the row containing the ignored check item, and click **Ignore** in the **Operation** column. Then, in the displayed dialog box, click **OK**.

----End

9.2 Vulnerability Management

9.2.1 Vulnerability Management Overview

Background

SecMaster integrates the vulnerability scanning data of Host Security Service (HSS) to centrally display asset vulnerability risks on the cloud, helping users detect asset security weaknesses in a timely manner and fix risky vulnerabilities.

SecMaster supports the following types of vulnerabilities:

- **ECS Vulnerabilities**
Reports vulnerabilities in Linux and Windows operating systems (OSs), Web-CMS vulnerabilities, and application vulnerabilities.

ECS Vulnerabilities

SecMaster can display host vulnerability scan information and vulnerability details, and provide vulnerability fixing suggestions.

The following host vulnerabilities can be detected:

Table 9-3 ECS vulnerability check items

Check Items	Description
Linux software vulnerability detection	SecMaster detects vulnerabilities in the system and software (such as SSH, OpenSSL, Apache, and MySQL) based on vulnerability libraries, reports the results to the management console, and generates alerts.
Windows OS vulnerability detection	SecMaster subscribes to Microsoft official updates, checks whether the patches on the server have been updated, pushes Microsoft official patches, reports the results to the management console, and generates vulnerability alerts.
Web-CMS vulnerability detection	SecMaster checks web directories and files for Web-CMS vulnerabilities, reports the results to the management console, and generates vulnerability alerts.

Check Items	Description
Application Vulnerabilities	SecMaster detects the vulnerabilities in the software and dependency packs running on the server, reports risky vulnerabilities to the console, and displays vulnerability alerts.

9.2.2 Viewing Vulnerability Details


View details about Linux, Windows, Web-CMS, and application vulnerabilities.

Prerequisites

- HSS logs have been connected to SecMaster and the function of automatically converting logs into alerts has been enabled. For details, see [Data Integration](#).

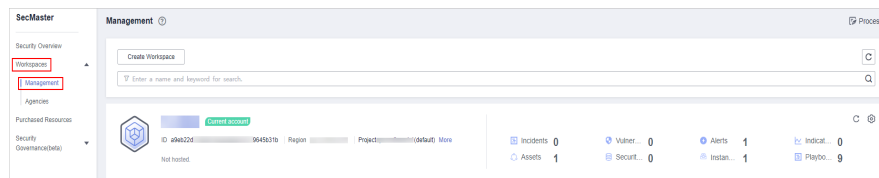
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

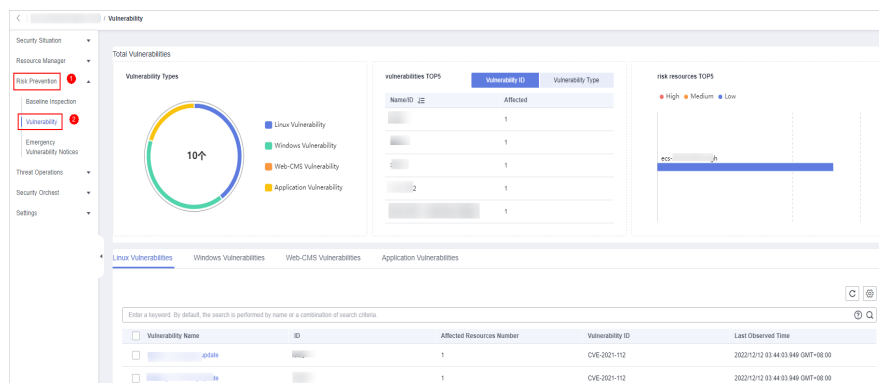
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-23 Management



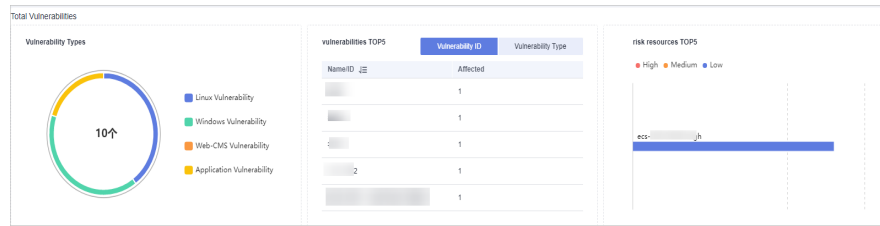
Step 4 In the navigation pane, choose **Risk Prevention > Vulnerabilities**.

Figure 9-24 Accessing the vulnerability management page




Step 5 Check vulnerability statistics.

Figure 9-25 Vulnerability statistics



- **Vulnerability Type Distribution:** displays the overall number of vulnerabilities and the distribution of each type of vulnerabilities.
- **Top 5 Vulnerabilities:** The **Vulnerability ID** tab displays the top 5 vulnerabilities with the largest number of vulnerability IDs and the number of affected assets. The **Vulnerability Type** tab displays the top 5 vulnerabilities with the largest number of vulnerability types, vulnerability risk levels, and affected assets.
- **Top 5 Vulnerable Resources:** displays top 5 risky assets.

Step 6 On the displayed page, click **Linux Vulnerabilities**, **Windows Vulnerabilities**, **Web-CMS Vulnerabilities**, or **Application Vulnerabilities**.

If there are a large number of vulnerabilities, you can specify the vulnerability name, vulnerability ID, severity, handling status and enter a keyword in the search box, and click  to quickly search for s specific vulnerability.

You can view a maximum of 9,999 vulnerability records on the page.

Table 9-4 Vulnerability parameters

Parameter	Description
Vulnerability Name	Name of the scanned vulnerability. Click a vulnerability name to view vulnerability description and vulnerability library information.
ID	Vulnerability ID
Affected Assets	Total number of assets affected by a vulnerability
Vulnerability ID	ID of a vulnerability.
Last Scan Time	Time of the last scan
Severity	Vulnerabilities are classified by risk severity, including Informational , Low , Medium , and High .

Step 7 To view details about a vulnerability, click the vulnerability name and view the details on the page that is displayed on the right.

----End

9.2.3 Fixing Vulnerabilities

This section describes how to fix vulnerabilities. The fixing method varies depending on the vulnerability type. Select a method based on the vulnerability type. The recommended fixing methods are as follows.

Table 9-5 Recommended fixing methods

Vulnerability Type	Recommended Fixing Method
Linux vulnerabilities	Use either of the following methods: <ul style="list-style-type: none"> • Use the repair function on the SecMaster console to fix the vulnerability. • Manually fix the vulnerability based on the suggestions provided on the console. Then, you can use the verification function to quickly check whether the vulnerability has been fixed.
Windows vulnerabilities	
Web-CMS vulnerabilities	Manually fix the vulnerability based on the suggestions provided on the console.
Application vulnerabilities	

CAUTION


- Vulnerability fixing operations cannot be rolled back. If a vulnerability fails to be fixed, services will probably be interrupted, and incompatibility issues will probably occur in middleware or upper-layer applications. To avoid unrecoverable errors, you are advised to use Cloud Server Backup Service (CSBS) to back up your servers. Then, use idle servers to simulate the production environment and test-fix the vulnerability. If the test-fix succeeds, fix the vulnerability on servers running in the production environment.
- Servers need to access the Internet and external image sources are used to fix vulnerabilities. If your servers cannot access the Internet, or the external image sources cannot provide stable services, you can use the image sources to fix vulnerabilities.

Before fixing vulnerabilities online, configure the image sources that match your server OSs.

Fixing Vulnerabilities on the Console

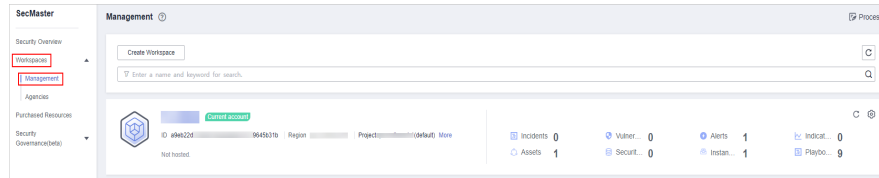
Only Linux vulnerabilities and Windows vulnerabilities can be fixed using the repair function on the console.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

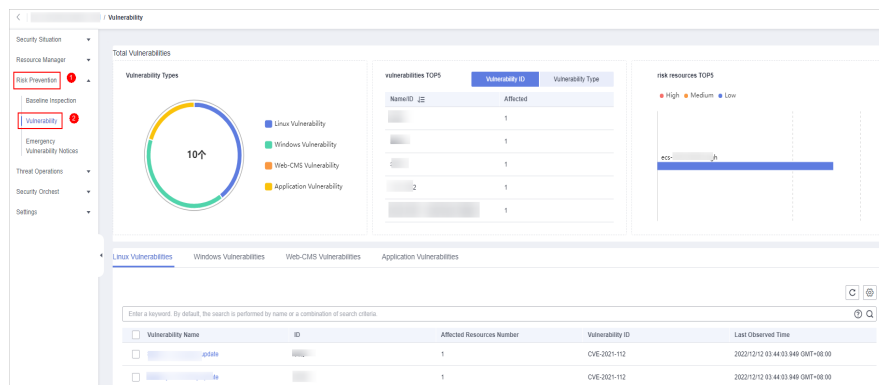
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-26 Management



Step 4 In the navigation pane, choose **Risk Prevention > Vulnerabilities**.

Figure 9-27 Accessing the vulnerability management page



Step 5 On the displayed page, click **Linux Vulnerabilities** or **Windows Vulnerabilities**.

Step 6 In the vulnerability list, click the name of the target vulnerability. The vulnerability details page is displayed.

Step 7 On the **Vulnerability Details** page, click **Affected Resources**. In the resource list, locate the row that contains the target resource and click **Repair** in the **Operation** column.

Step 8 If a vulnerability is fixed, its status will change to **Fixed**. If it fails to be fixed, its status will change to **Failed**.

NOTE

Restart the system after you fixed a Linux kernel vulnerability, or the system will probably continue to warn you of this vulnerability.

----End

Manually Fixing Software Vulnerabilities

- **Vulnerability Fixing Commands**

On the basic information page of vulnerabilities, you can fix a detected vulnerability based on the provided suggestions. For details about the vulnerability fixing commands, see [Table 9-6](#).

 **NOTE**

- Restart the system after you fixed a Windows or Linux kernel vulnerability, or the system will probably continue to warn you of this vulnerability.
- Fix the vulnerabilities in sequence based on the suggestions.
- If multiple software packages on the same server have the same vulnerability, you only need to fix the vulnerability once.

Table 9-6 Vulnerability fix commands

OS	Fix Command
CentOS/Fedora/ EulerOS/Red Hat/Oracle	yum update <i>Software name</i>
Debian/Ubuntu	apt-get update && apt-get install <i>Software name --only-upgrade</i>
Gentoo	See the vulnerability fix suggestions for details.

- **Vulnerability Fixing Methods**

Vulnerability fixing may affect service stability. You are advised to use either of the following methods to avoid such impacts:

- **Method 1: Create a VM to fix the vulnerability.**
 - i. Create an image for the ECS to be fixed.
 - ii. Use the image to create an ECS.
 - iii. Fix the vulnerability on the new ECS and verify the result.
 - iv. Switch services over to the new ECS and verify they are stably running.
 - v. Release the original ECS. If a fault occurs after the service switchover and cannot be rectified, you can switch services back to the original ECS.
- **Method 2: Fix the vulnerability on the current server.**
 - i. Create a backup for the ECS to be fixed.
 - ii. Fix vulnerabilities on the current server.
 - iii. If services become unavailable after the vulnerability is fixed and cannot be recovered in a timely manner, use the backup to restore the server.

 **NOTE**

- Use method 1 if you are fixing a vulnerability for the first time and cannot estimate the impact on services.
- Use method 2 if you have fixed the vulnerability on similar servers before.

Verifying Vulnerability Fix

After a vulnerability is fixed, you are advised to verify it immediately.

Table 9-7 Verification

Method	Operation
Manual verification	<ul style="list-style-type: none"> Click Verify on the vulnerability details page. Run the following command to check the software upgrade result and ensure that the software has been upgraded to the latest version: <ul style="list-style-type: none"> CentOS, Fedora, EulerOS, Red Hat, and Oracle: rpm -qa grep <i>Software name</i> Debian and Ubuntu: dpkg -l grep <i>Software name</i> Gentoo: emerge --search <i>Software name</i>
Automatic verification	HSS performs a full scan every early morning. If you do not perform a manual verification, you can view the system check result on the next day after you fix the vulnerability.

9.2.4 Importing and Exporting Vulnerabilities

This section describes how to import and export vulnerabilities.


- [Importing Vulnerabilities](#)
- [Exporting Vulnerabilities](#)

Constraints

Only .xlsx files no larger than 20 MB can be imported.

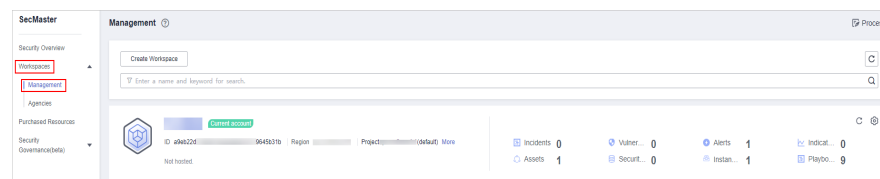
Importing Vulnerabilities

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

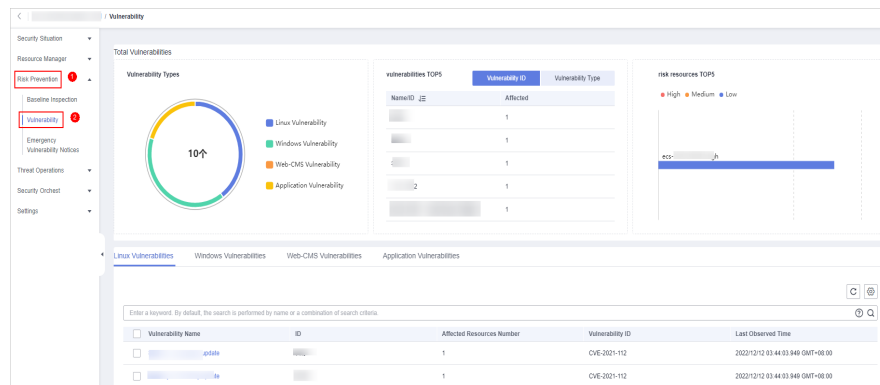
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-28 Management



Step 4 In the navigation pane, choose **Risk Prevention > Vulnerabilities**.

Figure 9-29 Accessing the vulnerability management page



Step 5 On the displayed page, click **Linux Vulnerabilities**, **Windows Vulnerabilities**, **Web-CMS Vulnerabilities**, or **Application Vulnerabilities**.

Step 6 Click **Import** above the vulnerability list. The **Import** dialog box is displayed.

Step 7 In the **Import** dialog box, click **Download Template** to download a template, and fill in the downloaded template according to the requirements.

CAUTION

- Provide vulnerability details based on the template. For details, see [Parameters in the Vulnerability Template](#).
- The file must be in the .xlsx format.

Step 8 After the vulnerability file is ready, click **Select File** in the **Import** dialog box, and select the Excel file you want to import.

Step 9 Click **OK**.

----End

Parameters in the Vulnerability Template

Import vulnerabilities based on the template requirements. For details about the parameters, see [Table 9-8](#).

Table 9-8 Parameters in the vulnerability template

Parameter	Type	Mandatory	Description
vul_name_zh	String	Yes	Chinese name of the vulnerability. The value contains a maximum of 255 characters.

Parameter		Type	Mandatory	Description
vul_name_en		String	Yes	English name of the vulnerability. The value contains a maximum of 255 characters.
vul_name		String	Yes	Vulnerability name. The value contains a maximum of 255 characters.
resource		Object	Yes	Affected resources. Example: <pre>{ "domain_id":"f9d7bacbfd2c49e892532ba3f62ab75d", "provider":"ecs", "project_id":"f69081793d9e4ea8a2f479dcef961989", "name":"WAF_12345678-T5Q3", "region_id":"xxx", "id":"964b692a-8a89-488c-bf65-2bd6fd6f36f7", "type":"cloudservers", "ep_id":null, "tags":{"ip":"192.168.0.116", "high_risk_port":"20" }}</pre>
resource	id	String	Yes	Cloud service resource ID.
	name	String	Yes	Resource name. The value contains a maximum of 255 characters.
	type	String	Yes	Resource type.
	provider	String	Yes	Cloud service name.
	region_id	String	No	Region ID.
	domain_id	String	Yes	ID of the account to which the resource belongs.
	project_id	String	No	ID of the project to which the resource belongs.
	ep_id	String	No	Enterprise project ID.
	ep_name	String	No	Enterprise project name.

Parameter		Type	Mandatory	Description
	tags	Object	No	Resource tags. <ul style="list-style-type: none"> A maximum of 50 key-value pairs are supported. The value contains a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _ , ; , /, @).
remediation		Object	No	Remediation measures. Example: <pre>{ "recommendation": "The official advisory for this vulnerability has been released, please click the following links to fix it according to the suggestions: \nhttps://bugzilla.redhat.com/show_bug.cgi?id=1691529\nThe patch for this vulnerability can be referred to:\nhttps://go.golangsource.com/crypto//b7391e95e576caccdd422573063bc057239113d\nThe third party advisory for this vulnerability can be referred to:\nhttps://groups.google.com/forum/#!msg/golang-announce/tjyNcJxb2vQ/n0NRBziSCAAJ\nhttps://github.com/golang/go/issues/30965\nThe exploit/POC for this vulnerability has been exposed, for verification please refer to:\nhttps://github.com/Live-Hack-CVE/CVE-2019-11840\n"} </pre>
remediation	recommendation	String	No	Recommended solution.
	url	String	No	Link to the general fix information for the vulnerability. The URL must be accessible from the public network. No credential is required.
environment		Object	Yes	Coordinates of the environment where the vulnerability is generated.
environment	vendor_type	string	Yes	Environment vendor.
	domain_id	String	Yes	Account ID.

Parameter		Type	Mandatory	Description
	region_id	String	Yes	Region ID..
	project_id	String	No	Project ID. The default value is null for global services.
data_source		Object	Yes	Data source reported for the first time.
data_source	source_type	Int	Yes	Data source type.
	domain_id	String	Yes	ID of the account to which the data source product belongs. The value contains a maximum of 36 characters.
	project_id	String	Yes	ID of the project to which the data source product belongs. The value contains a maximum of 36 characters.
	region_id	String	Yes	Region where the data source product is located.
	company_name	String	Yes	Name of the company to which the data source product belongs. The value contains a maximum of 16 characters.
	product_name	String	Yes	Name of the data source product. The value contains a maximum of 24 characters.
	product_feature	String	Yes	Name of the product function or feature. The value contains a maximum of 24 characters.
	product_module	String	No	List of the detection modules.
workspace_id		String	Yes	Workspace ID.

Parameter	Type	Mandatory	Description
arrive_time	Timestamp	Yes	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the vulnerability was received. If this parameter cannot be parsed, the default time zone GMT+8 is used. Example: 2023-03-30T12:14:50.472Z+0800
source_url	String	No	Vulnerability URL, which points to the page of the current vulnerability description in the data source product.
description_zh	String	Yes	Vulnerability description in Chinese. The value contains a maximum of 1024 characters.
description_en	String	Yes	Vulnerability description in English. The value contains a maximum of 1024 characters.
description	String	Yes	Vulnerability description. The value contains a maximum of 1024 characters.
close_reason	String	No	Closure reason. The value can be False detection , Resolved , Repeated , or Other .
close_comment	String	No	Comment for the closure.

Parameter	Type	Mandatory	Description
create_time	Times tamp	Yes	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms +Time zone". Time zone refers to where the vulnerability was recorded. If this parameter cannot be parsed, the default time zone GMT+8 is used. Example: 2023-03-30T12:14:50.473Z +0800
close_time	Times tamp	No	Closing time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms +Time zone". Time zone refers to where the vulnerability was closed. If this parameter cannot be parsed, the default time zone GMT+8 is used. Example: 2023-03-30T12:14:50.472Z +0800
update_time	Times tamp	No	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms +Time zone". Time zone refers to where the vulnerability was updated. If this parameter cannot be parsed, the default time zone GMT+8 is used. Example: 2023-03-30T12:14:50.472Z +0800
criticality	Int	No	Importance level of the resource involved in the vulnerability. Value range: 0–100. 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.

Parameter	Type	Mandatory	Description
close_method	String	No	Closing method. The value can be: <ul style="list-style-type: none"> • soc_auto: The vulnerability is fixed automatically. • soc_manual: SecMaster triggers the closure via the playbook. • hss_manual: HSS triggers the closure. • csb_manual: SecMaster triggers the closure directly.
batch_number	String	Yes	Batch number, which is used to mark and compare exploits of the vulnerability.
history_observed_source	List<String>	No	Historically reported data sources: HSS and VSS.
count	Int	Yes	Number of vulnerability occurrences.
first_observed_time	Timestamp	Yes	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the vulnerability was discovered for the first time. If this parameter cannot be parsed, the default time zone GMT+8 is used. Example: 2023-03-30T12:14:50.473+08:00

Parameter	Type	Mandatory	Description
last_observed_time	Timestamp	Yes	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the vulnerability was discovered recently. If this parameter cannot be parsed, the default time zone GMT+8 is used. Example: 2023-03-30T12:14:50.473Z+0800
id	String	Yes	Unique identifier of the vulnerability. The value is in the UUID format and contains a maximum of 36 characters.
version	String	Yes	Version of the vulnerability object.
handled	String	Yes	Whether the vulnerability is handled.
domain_id	String	Yes	ID of the account to which the resource belongs.
region_id	String	Yes	Region ID.

Parameter	Type	Mandatory	Description
vulnerability	Object	Yes	<p>Vulnerability information. The following is an example:</p> <pre> { "reason":"Offline Processing", "solution_en":"The official advisory for this vulnerability has been released, please click the following links to fix it according to the suggestions: \nhttps://bugzilla.redhat.com/show_bug.cgi?id=1691529\nThe patch for this vulnerability can be referred to:\nhttps://go.golangsource.com/crypto//b7391e95e576caccdd422573063bc057239113d\nThe third party advisory for this vulnerability can be referred to:\nhttps://groups.google.com/forum/#!msg/golang-announce/tjyNcJxb2vQ/n0NRBziSCAAJ\nhttps://github.com/golang/go/issues/30965\nThe exploit/POC for this vulnerability has been exposed, for verification please refer to:\nhttps://github.com/Live-Hack-CVE/CVE-2019-11840\n", "last_observed_time":"2023-03-23T14:31:41.42108:00", "level":"Medium", "type":3, "url":["https://go.golangsource.com/crypto//b7391e95e576caccdd422573063bc057239113d"], "repair_severity":2, "related":["CVE-2019-11840"], "solution":"The official fixing suggestions for this vulnerability have been released. You can visit the link to fix the vulnerability accordingly: \nhttps://bugzilla.redhat.com/show_bug.cgi?id=1691529\n For details about the patch for this vulnerability, see: \nhttps://go.golangsource.com/crypto//b7391e95e576caccdd422573063bc057239113d\n For details about the non-official fixing suggestions for this vulnerability, see: \nhttps://groups.google.com/forum/#!msg/golang-announce/tjyNcJxb2vQ/n0NRBziSCAAJ\nhttps://github.com/golang/go/issues/30965\n Exploit/POC for this vulnerability has been exposed. You can visit the following link for verification: \nhttps://github.com/ </pre>

Parameter		Type	Man dator y	Description
				<pre> Live-Hack-CVE/ CVE-2019-11840\n", "solution_en":"The official fixing suggestions for this vulnerability have been released. You can visit the link to fix the vulnerability accordingly: \nhttps:// bugzilla.redhat.com/show_bug.cgi? id=1691529\n For details about the patch for this vulnerability, see: \nhttps:// go.googleusercontent.com/crypto// b7391e95e576caccdd422573063b c057239113d\n For details about the non-official fixing suggestions for this vulnerability, see: \nhttps:// groups.google.com/forum/#!msg/ golang-announce/tjyNcJxb2vQ/ n0NRBziSCAAJ\nhttps:// github.com/golang/go/issues/ 30965\n Exploit/POC for this vulnerability has been exposed. You can visit the following link for verification: \nhttps://github.com/ Live-Hack-CVE/ CVE-2019-11840\n", "comment":null, "id":"HCVD-APP- CVE-2019-12345", "status":4 } </pre>
vulnerabil ity	id	String	Yes	Vulnerability ID. CAUTION The ID must be unique globally.
	type	Int	Yes	Vulnerability type. <ul style="list-style-type: none"> ● 0: Linux ● 1: Windows ● 2: Web-CMS ● 3: application ● 4: website ● 5: others
	level	String	Yes	Vulnerability level. The value can be High , Medium , Low , or Hint .
	tags	List<String>	No	Vulnerability tags.
	solution	String	No	Vulnerability fixing solution.
	url	String	No	URL information.


Parameter		Type	Mandatory	Description
	related	List<String>	Yes	Associated CVE IDs.
	repair_severity	Int	Yes	Repair urgency. <ul style="list-style-type: none"> 0: high 1: medium 2: low 3: hint
	status	Int	Yes	Repair status. <ul style="list-style-type: none"> 0: unfix 1: ignored 2: verified 3: fixing 4: fixed 5: reboot 6: failed
	reason	String	No	Status change reason.
	comment	String	No	Other comments for status change.
	apps	List<Object>	No	List of involved software.
apps	name	String	Yes	Software name.
	version	String	Yes	Software version.
	image_name	String	No	Image.
	upgrade_version	String	Yes	Fixed version.
	path	String	No	Path of the software.
	match_detail	String	No	Hit details.
	match_rule	String	No	Hit rule.
	pid	String	No	Process ID.
	repair_cmd	String	No	Fix command.

Parameter		Type	Mandatory	Description	
	need_boot	int	No	Whether to restart the server. <ul style="list-style-type: none"> • 1: true • 0: false 	
	domain	Object	No	Website vulnerability information.	
	domain	url	String	Yes	URL.
		poc	String	No	Hit details, attack fields, and alert information.
		request	String	No	Test request packet.
		response	String	No	Test response packet.
playbook_name		String	No	Playbook name.	
resource_num		int	Yes	Resource quantity.	

Exporting Vulnerabilities

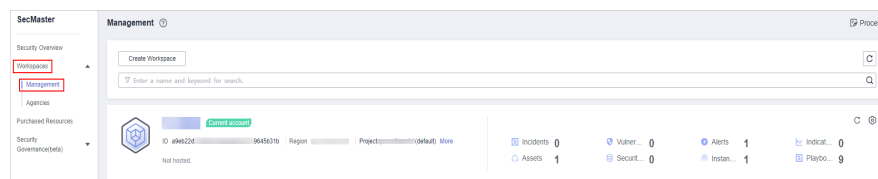
A maximum of 9,999 vulnerability records can be exported.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

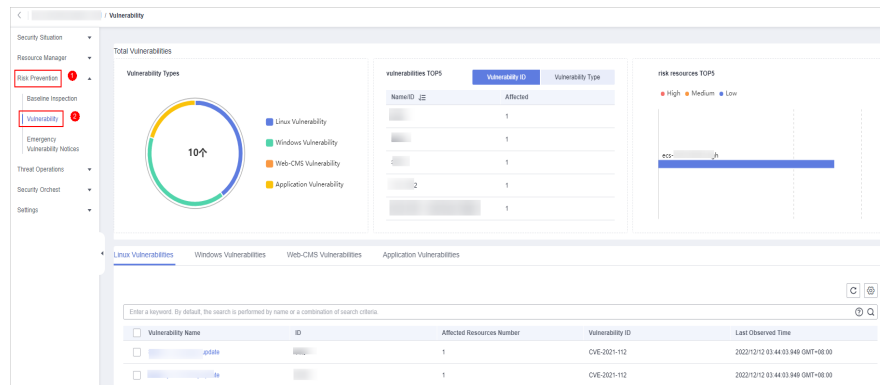
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-30 Management




Step 4 In the navigation pane, choose **Risk Prevention > Vulnerabilities**.

Figure 9-31 Accessing the vulnerability management page



Step 5 On the displayed page, click **Linux Vulnerabilities, Windows Vulnerabilities, Web-CMS Vulnerabilities, or Application Vulnerabilities.**

Step 6 Click  in the upper right corner above the vulnerability list. The **Export** dialog box is displayed.

Step 7 In the **Export** dialog box, set vulnerability parameters.

Table 9-9 Exporting vulnerabilities

Parameter	Description
Format	By default, the vulnerability list is exported into an Excel.
Columns	Select the parameters included in the exported file.

Step 8 Click **OK**.

The system automatically downloads the Excel to your local PC.

----End


9.2.5 Ignoring and Unignoring a Vulnerability

Some vulnerabilities are risky only in specific conditions. For example, if a vulnerability can be exploited only through an open port, but the target server does not open any ports, the vulnerability will not harm the server. Such vulnerabilities can be ignored. After a vulnerability is ignored, no alerts will be reported for the vulnerability.

This topic describes how to ignore a vulnerability and cancel ignoring a vulnerability.

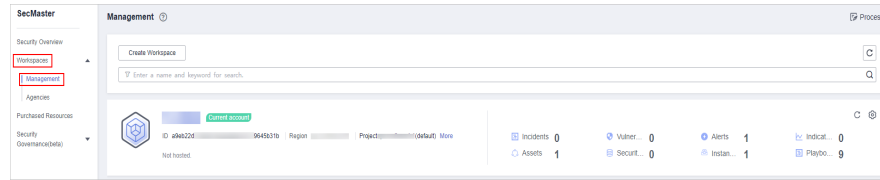
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

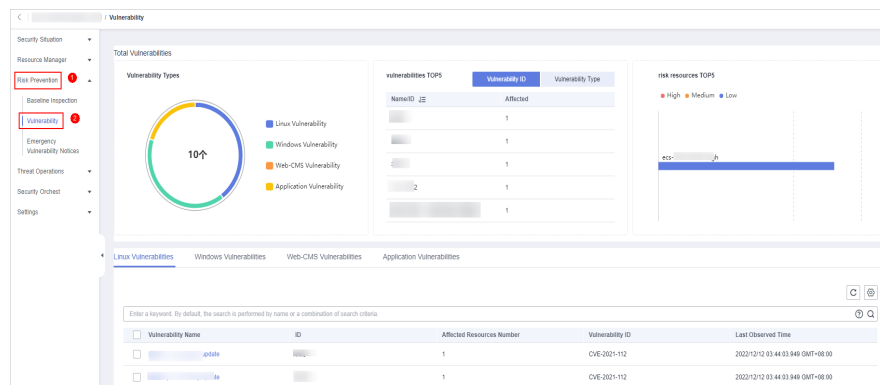
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 9-32 Management



Step 4 In the navigation pane, choose **Risk Prevention > Vulnerabilities**.

Figure 9-33 Accessing the vulnerability management page



Step 5 On the displayed page, click **Linux Vulnerabilities**, **Windows Vulnerabilities**, **Web-CMS Vulnerabilities**, or **Application Vulnerabilities**.

Step 6 In the vulnerability list, click the name of the target vulnerability. The vulnerability details page is displayed.

Step 7 Ignore or unignore the target vulnerability.

- Ignore

On the **Vulnerability Details** page, click **Affected Resources**. In the resource list, locate the row that contains the target resource and click **More** and then **Ignore** in the **Operation** column.

- Unignore

a. On the **Vulnerability Details** page, click **Affected Resources**. In the resource list, locate the row that contains the target resource and click **More** and then **Cancel Ignore** in the **Operation** column.

b. In the confirmation dialog box, confirm the information and click **OK**.

----End

10 Threat Operations

10.1 Incident Management

10.1.1 Viewing an Incident

By viewing the incident list, you can learn about the incident statistics in the last 360 days. The list contains the incident name, type, severity, and occurrence time. By customizing filtering conditions, such as the incident name, risk severity, and time, you can quickly query information about the specific incident.

This topic describes how to view incident information.

Procedure


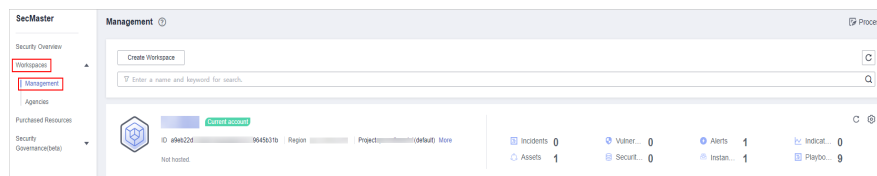
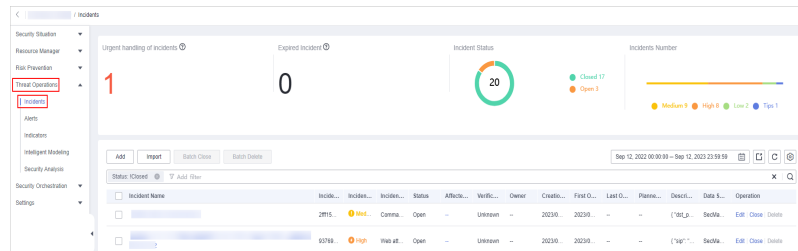
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-1 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Incidents**.

Figure 10-2 Incidents



Step 5 In the upper part of the **Incidents** page, view incident statistics.

Figure 10-3 Incident statistics



- **Urgent handling of Incidents:** displays the total number of critical or high-risk incidents that are not closed.
- **Expired Incident:** displays the total number of incidents that have not been closed after the planned closure time set for the incidents.
- **Incident Status:** displays the total number of incidents in the **Open**, **Blocked**, and **Closed** statuses and the number of incidents in the corresponding status.
- **Total Incidents:** Total number of incidents in the current workspace and the number of incidents of each severity.

Step 6 In the incident list, view the incident details. For details about the parameters, see [Viewing an Incident](#).

You can view a maximum of 9,999 incidents on the page.

Table 10-1 Incident parameters

Parameter	Description
Incident	Incident name.
Incident ID	ID of an incident.
Incident Level	Severity level. The options are Warning , Low-risk , Medium-risk , High-risk , and Critical .
Type	Incident type
Status	Incident status. The options are Open , Blocked , and Closed .
Affected Asset	Assets affected by this incident.
Verification Status	Verification status of the incident, that is, the accuracy of the incident. The value can be Unknown, Acknowledged, or False Alarm.
Owners	Primary owner of the incident.
Created	Time when the incident is created.

Parameter	Description
First occurrence time	First Occurrence Time
Last occurrence time	Time when the incident occurred last time.
Planned Closure Date	Planned closure time of the incident.
Description	A brief description of the incident
Data Source Product Name	Name of the product from which an incident is generated.
Labels	Incident label.
Operation	You can edit or close an incident.

Step 7 To view details about an incident, click the incident name. The incident details are displayed on the right of the page.


----End

10.1.2 Adding or Editing an Incident

This section describes how to add or edit an incident.

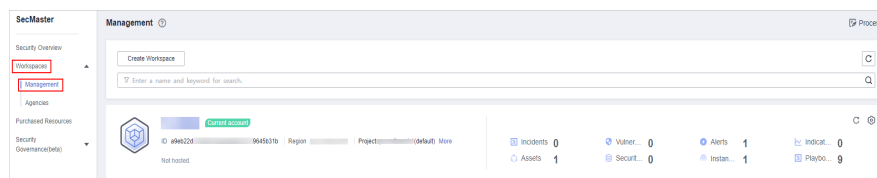
Adding an Incident

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

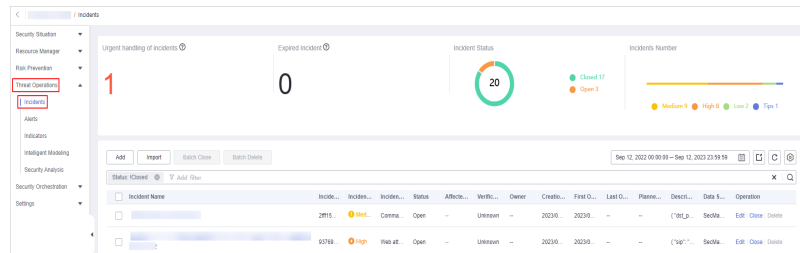
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-4 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Incidents**.

Figure 10-5 Incidents



Step 5 On the **Incidents** page, click **Add**. On the displayed **Add** page, set parameters as described in [Table 10-2](#).

Table 10-2 Parameters for adding an incident

Parameter		Description
Basic Information	Incident Name	Custom incident name. The value must contain: <ul style="list-style-type: none"> Only uppercase letters, lowercase letters, digits, and the special characters: - _ () A maximum of 255 characters
	Incident Type	Incident type
	(Optional) Service ID	Enter the service ID corresponding to the incident.
	Incident Level	Severity level. The options are Tips , Low , Medium , High , and Fatal .
	Status	Incident status. The options are Open , Blocked , and Closed .
	Data Source Name	Data source name
	Data Source Type	Type of the data source.
	(Optional) Owner	Primary owner of the incident.
Timeline	First Occurrence Time	Time when the incident occurred first time.
	(Optional) Last Occurrence Time	Time when the incident occurred last time.
	(Optional) Planned Closure Time	Time to close the incident.


Parameter		Description
Other	(Optional) Verification Status	Verification status of the incident to identify the accuracy of the incident. The options are Unknown , Positive , and False positive .
	(Optional) Stage	Incident phase. <ul style="list-style-type: none"> ● Preparation: Prepare resources to process incidents. ● Detection and analysis: Detect and analyze the cause of an incident. ● Contain, extradition, and recovery: Handle an incident. ● Post Incident Activity: Follow-up activities.
	(Optional) Debugging data	Whether to enable simulated debugging
	(Optional) Label	Label of the incident.
	Description	Incident description. The value can contain: <ul style="list-style-type: none"> ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 1,024 characters.

Step 6 Click **OK**. The incident is created.

----End

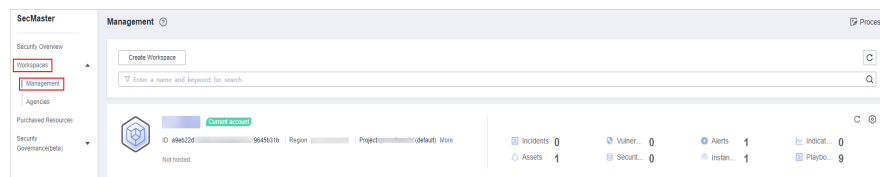
Editing an Incident

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

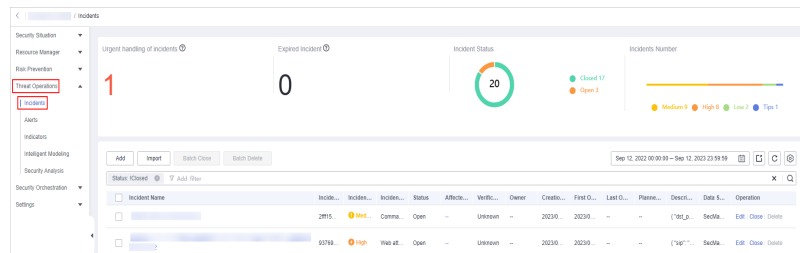
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-6 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Incidents**.

Figure 10-7 Incidents



Step 5 In the incident list, locate the row that contains the target incident and click **Edit** in the **Operation** column.

Step 6 On the **Edit** page that is displayed, edit incident parameters.

Table 10-3 Parameters for editing an incident

Parameter		Description
Basic Information	Incident Name	Custom incident name. The value must contain: <ul style="list-style-type: none"> Only uppercase letters, lowercase letters, digits, and the special characters: - _ () A maximum of 255 characters
	Incident Type	Incident type
	(Optional) Service ID	Enter the service ID corresponding to the incident.
	Incident Level	Severity level. The options are Tips , Low , Medium , High , and Fatal .
	Status	Incident status. The options are Open , Blocked , and Closed .
	Data Source Name	Name of the data source, which cannot be changed
	Data Source Type	Type of the data source, which cannot be changed
(Optional) Owner	Primary owner of the incident.	
Timeline	First Occurrence Time	Time when the incident occurred first time.
	(Optional) Last Occurrence Time	Time when the incident occurred last time.
	(Optional) Planned Closure Time	Time to close the incident.
Other	(Optional) Verification Status	Verification status of the incident to identify the accuracy of the incident. The options are Unknown , Positive , and False positive .

Parameter		Description
	(Optional) Phase	Incident phase. <ul style="list-style-type: none"> ● Preparation: Prepare resources to process incidents. ● Detection and analysis: Detect and analyze the cause of an incident. ● Contain, extradition, and recovery: Handle an incident. ● Post Incident Activity: Follow-up activities.
	(Optional) Debugging data	Whether to enable simulated debugging. This parameter cannot be modified once configured.
	(Optional) Label	Label of the incident.
	Description	Incident description. The value can contain: <ul style="list-style-type: none"> ● Only uppercase letters, lowercase letters, digits, and the special characters: - _ () ● A maximum of 1,024 characters.

Step 7 Click **OK**. The incident editing is complete.

----End

10.1.3 Importing and Exporting Incidents


This section describes how to import incidents.

Limitations and Constraints

Only .xlsx files no larger than 20 MB can be imported.

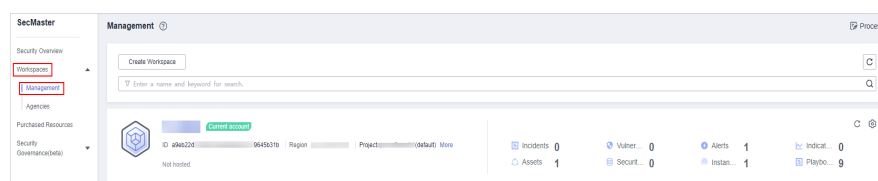
Importing Incidents

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

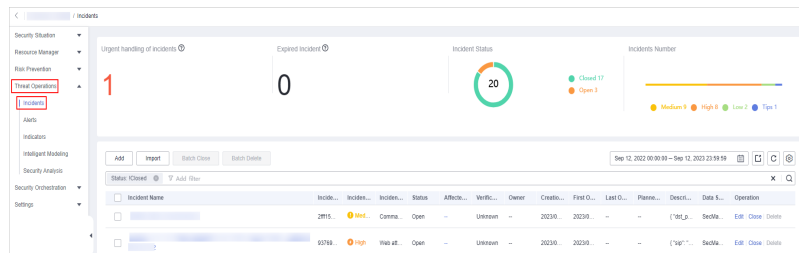
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-8 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Incidents**.

Figure 10-9 Incidents



Step 5 On the **Incidents** page, click **Import** in the upper left corner above the incident list.

Step 6 In the displayed **Import** dialog box, click **Download Template** to download a template, and fill in the downloaded template according to the requirements.

Step 7 After the template is filled, click **Add File** in the **Import Incident** dialog box and select the Excel file you want to import.

CAUTION

- Fill in information about incidents to be imported based on the template. For details, see [Parameters in the Incident Template](#).
- The file must be in the .xlsx format.

Step 8 Click **OK**.

----End

Parameters in the Incident Template

Import incidents based on the template requirements. For details about the parameters, see [Table 10-4](#).

Table 10-4 Parameters in the incident template

Parameter	Type	Mandatory	Description
extend_properties	Object	No	Extended properties of the incident.
ttr	Int	No	Response time of the incident.
ttd	Int	No	Time when the incident is detected.
ref_order_id	String	No	Service ID (service ticket ID) of the incident. The value contains a maximum of 128 characters.

Parameter	Type	Mandatory	Description
region_id	String	Yes	Region ID of the tenant to which the incident object belongs.
domain_id	String	Yes	Domain ID of the tenant to which the incident object belongs.
origin_id	String	No	Origin ID of the incident. The value contains a maximum of 128 characters.
file_info	List<object >	No	File information.
user_info	List<object >	No	User information.
process	List<object >	No	Process information.
incident_type	Object	Yes	Incident type. Example: {"incident_type":"demo","id":"demo"}
network_list	List[Object]	No	Network information.
resource_list	List[Object]	No	Affected resources.
malware	Object	No	Malware.
system_info	Object	No	System information.
data_source	Object	Yes	Data source. Example: {"REGION_ID":"demo","product_feature":"demo","project_id":"demo","product_module":"demo","company_name":"demo","DOMAIN_ID":"demo","source_type":445428683,"product_name":"demo"}
remediation	Object	No	Remediation measures.
is_deleted	Boolean	No	Whether to delete the incident.
environment	Object	Yes	Coordinates of the environment where the incident is generated.
workspace_id	String	Yes	ID of the workspace to which the incident object belongs.
sla	Int	No	SLA for closing the incident, in hours. This parameter sets the duration in which risks can be accepted.

Parameter	Type	Mandatory	Description
close_time	Timestamp	No	Closing time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident was closed. If this parameter cannot be parsed, the default time zone GMT+8 is used.
owner	String	No	Owner and service owner.
close_comment	String	No	Comment for the closure.
count	Int	Yes	Incident occurrences.
close_reason	String	No	Closure reason. The value can be: <ul style="list-style-type: none"> • False detection • Resolved • Repeated • Other
handle_status	String	Yes	Incident processing status. The value can be: <ul style="list-style-type: none"> • Open: opened • Block: blocked • Closed: closed The default value is Open .
update_time	Timestamp	No	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident was updated. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	Timestamp	Yes	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident was recorded. If this parameter cannot be parsed, the default time zone GMT+8 is used. Example: 2023-04-13T10:36:20.580Z+0800

Parameter	Type	Mandatory	Description
first_observed_time	Timestamp	Yes	First occurrence time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	Timestamp	Yes	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident was received. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	Timestamp	No	Latest occurrence time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident recently occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
description	String	Yes	Incident description. The value contains a maximum of 1024 characters.
ipdrr_phase	String	No	Period/Phase number.
title	String	Yes	Incident name. The value contains a maximum of 255 characters.
confidence	Int	No	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or event. Value range: 0–100 <ul style="list-style-type: none"> ● 0: The incident confidence is 0%. ● 100: The incident confidence is 100%.

Parameter	Type	Mandatory	Description
verification_state	String	Yes	<p>Verification status, used to identify the accuracy of the incident.</p> <ul style="list-style-type: none"> • Unknown: The status is unknown. • True_Positive: The status is confirmed. • False_Positive: The status is false positive. <p>The default value is Unknown.</p>
version	String	Yes	Version of the incident object.
actor	String	No	Incident investigator.
creator	String	No	Creator.
simulation	Boolean	No	Debugging field.
severity	String	Yes	<p>Incident level. The value can be:</p> <ul style="list-style-type: none"> • Tips: No threat is found. • Low: No operation is required for the threat. • Medium: The threat needs to be handled but is not urgent. • High: The threat must be handled preferentially. • Fatal: The threat must be handled immediately to prevent further damage.
criticality	Int	No	<p>Importance level of the resource involved in the incident.</p> <p>Value range: 0–100. 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.</p>
source_url	String	No	Incident URL, which points to the page of the current incident description in the data source product.
id	String	Yes	<p>Unique identifier of the incident. The value is in the UUID format and contains a maximum of 36 characters.</p>
labels	String	No	Labels.

Exporting Incidents


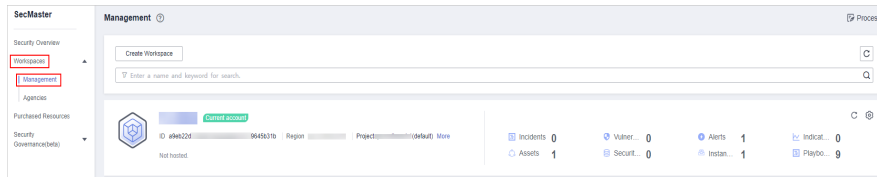
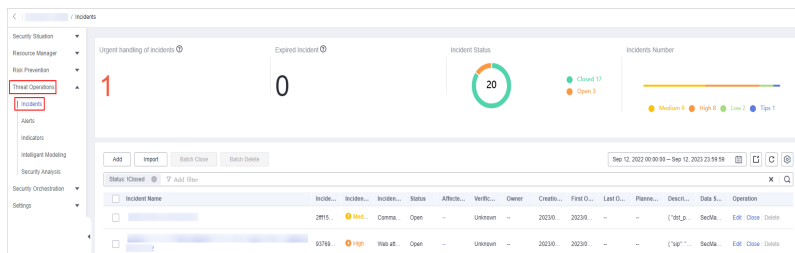
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-10 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Incidents**.

Figure 10-11 Incidents




- Step 5** On the **Incidents** page, select the incidents to be exported and click  in the upper right corner of the list. The **Export** dialog box is displayed.
- Step 6** In the **Export** dialog box, set parameters.

Table 10-5 Exporting incidents

Parameter	Description
Format	By default, the incident list is exported into an Excel.
Columns	Select the parameters to be exported.

- Step 7** Click **OK**.
The system automatically downloads the Excel to your local PC.
- End

10.1.4 Closing or Deleting Incidents

This section describes how to perform the following operations: **Closing an Incident** and **Deleting an Incident**.

Closing an Incident


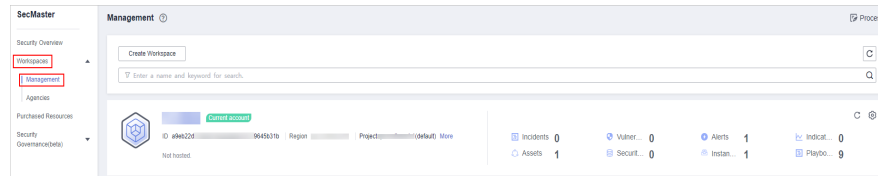
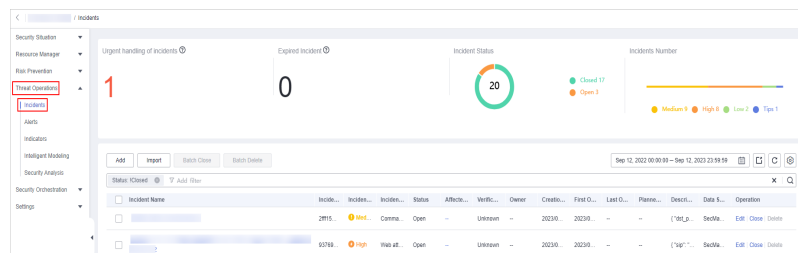
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-12 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Incidents**.

Figure 10-13 Incidents



- Step 5** In the incident management list, locate the row that contains the target incident, click **Close** in the **Operation** column.
- Step 6** In the confirmation dialog box, select **Reason for**, enter **Close Comment**, and click **OK**.

----End

Deleting an Incident


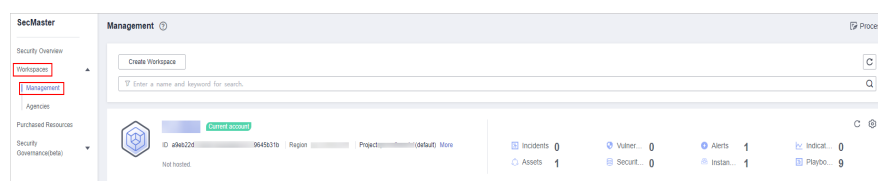
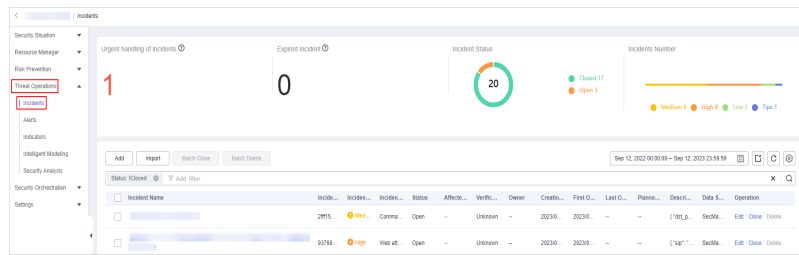
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-14 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Incidents**.

Figure 10-15 Incidents



Step 5 On the **Incident** page, locate the row that contains the target incident and click **Delete** in the **Operation** column.

Step 6 In the dialog box that is displayed, click **OK**.

NOTE

Deleted incidents cannot be restored. Exercise caution when performing this operation.

----End

10.2 Alert Management


10.2.1 Viewing Alerts

On the **Alerts** tab, you can query alerts in the last 180 days. You can view the alert details, including alert name, type, risk severity, and generation time. By customizing filtering conditions, such as the alert name, risk severity, and time, you can quickly query information about the specific alerts.

This section describes how to view alert information.

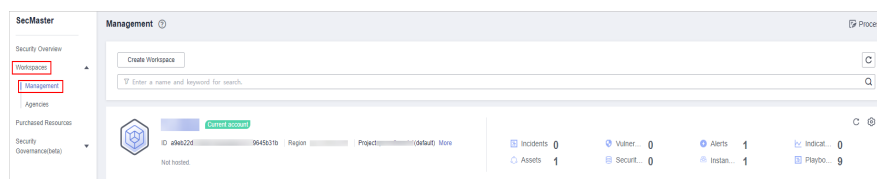
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

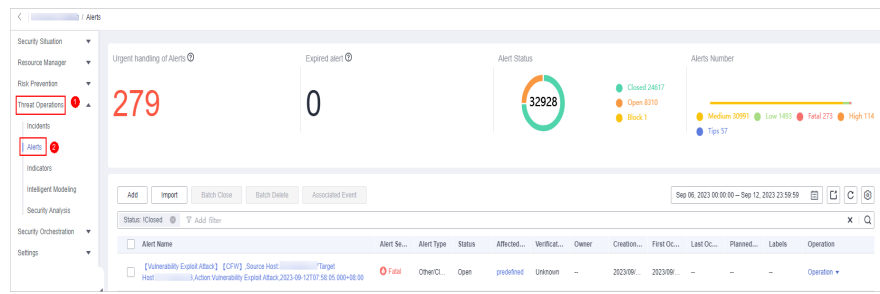
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-16 Management



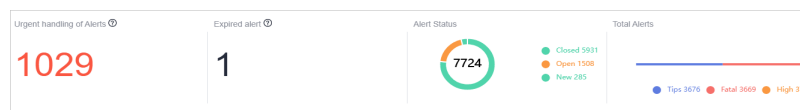
Step 4 In the navigation pane on the left, choose **Threat Operations > Alerts**.

Figure 10-17 Alerts



Step 5 In the upper part of the Alerts page, view alert statistics.

Figure 10-18 Alert statistics



- **Urgent handling of Alerts:** displays the total number of critical or high-risk alerts that are not closed.
- **Expired Alerts:** displays the total number of alerts that have not been closed after the planned closure time.
- **Alert Status:** displays the total number of alerts in **Open**, **Block**, and **Closed** statuses, and the number of alerts in each status.
- **Total Alerts:** displays the total number of alerts in the current workspace and the number of alerts of each severity.

Step 6 On the Alerts page, view alert details. For details about the parameters, see [Table 10-6](#).

You can view a maximum of 9,999 alert records on the page.

Table 10-6 Alert parameters

Parameter	Description
Alert Name	Indicates the name of the alert.
Alert Severity	Alert severity. The options are Tips , Low , Medium , High , and Fatal .
Alert Type	Alert type.
Status	Alert status. The options are Open, Blocked, and Closed.
Affected Assets	Assets affected by the alert. You can move the mouse pointer to the name of an affected asset to view the asset details.
Verification Status	Verification status of the alert, that is, the accuracy of the incident. The options are Unknown , Positive , and False positive .

Parameter	Description
Owner	Indicates the primary owner of the alert.
Creation Time	Time when the alert is created.
First Occurrence Time	Time when the alert is generated for the first time.
Last Occurrence Time	Last time when an alert was generated
Planned Closure Time	Indicates the planned time when the alert is closed.
Labels	Labels of the alert.
Operation	You can edit, close, and delete alerts.

Step 7 To view the overview of an alert, click the alert name. The alert overview is displayed on the right.

- On the alert overview page, you can view alert handling suggestions, basic information, and associated information (including associated threat metrics, alerts, incidents, and attack information).
- To view alert details, click **Alert Details** in the lower right corner of the alert overview page. The alert details page is displayed.
On the details page, you can view the alert timeline and attack information in addition to the information on the overview page. For example, you can view the first occurrence time of an alert, detection time, and attack process ID.
- On the alert overview or details page, you can change the alert severity and status in the alert severity and status drop-down list boxes.
- On the alert overview or details page, you can associate or disassociate alerts and incidents and view information about affected resources.


----End

10.2.2 Converting an Alert to an Incident

This section describes how to convert an alert to an incident.

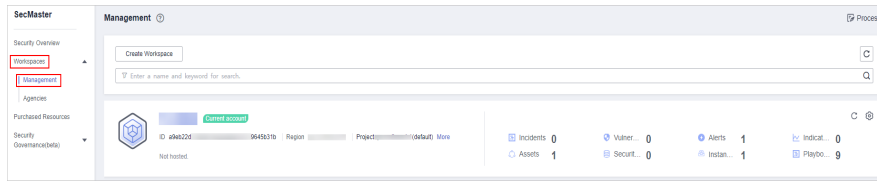
Converting an Alert to an Incident

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

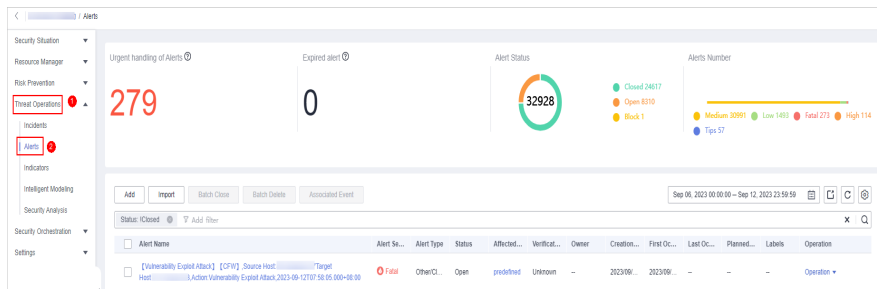
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-19 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Alerts**.

Figure 10-20 Alerts

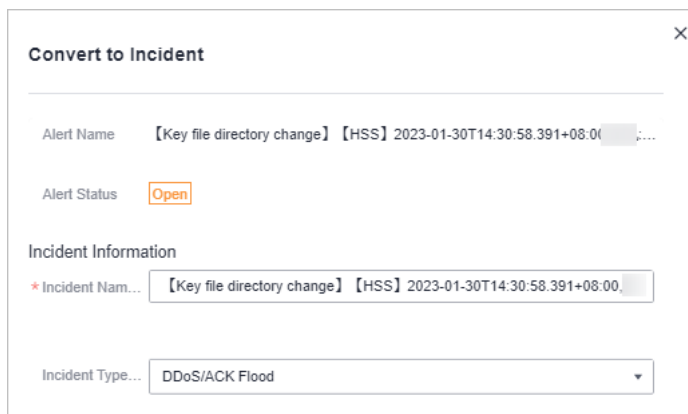


Step 5 In the alert list, locate the row that contains the target alert, click **Convert to Incident** in the **Operation** column. The **Convert to Incident** page is displayed on the right.

Step 6 On the displayed page, set the **Incident Type**. Retain the default settings for other parameters.

The incident name is automatically set to the name of the current alert and can be modified.

Figure 10-21 Converting an alert to an incident



Step 7 Click **OK**.


----End

10.2.3 Adding or Editing an Alert

This section describes how to add or edit an alert.

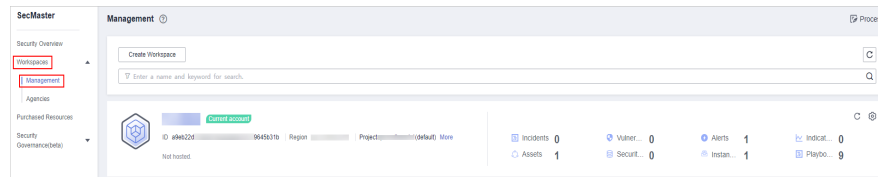
Adding an Alert

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

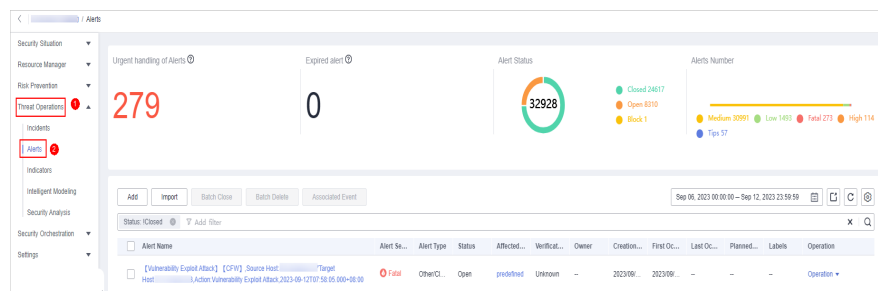
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-22 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Alerts**.

Figure 10-23 Alerts



Step 5 On the **Alerts** page, click **Add**. On the **Add** page displayed on the right, set parameters as described in [Table 10-7](#).

Table 10-7 Alert parameters

Parameter		Description
Basic information	Alert Name	User-defined alert name. The value must contain: <ul style="list-style-type: none"> Only uppercase letters, lowercase letters, digits, and the special characters: - _ () A maximum of 255 characters
	Alert Type	Alert type
	Alert Severity	Alert severity. The options are Tips , Low , Medium , High , and Fatal .
	Status	Alert status. The options are Open , Blocked , and Closed .
	(Optional) Owner	Primary owner of the alert.


Parameter		Description
	Data Source Product Name	Data source name
	Data Source Type	Type of the data source.
Timeline	First Occurrence Time	Time when an alert is generated for the first time.
	(Optional) Last Occurrence Time	Last time when an alert was generated
	(Optional) Planned Closure Time	Time when the alert plan is disabled.
Other	(Optional) Labels	Alert labels.
	(Optional) Debugging data	Whether to enable simulated debugging.
	(Optional) Verification Status	Verification status of the alert to identify the accuracy of the incident. The options are Unknown , Positive , and False positive .
	(Optional) Stage	Alert phase. <ul style="list-style-type: none"> ● Preparation: Prepare resources to process alert. ● Detection and analysis: Detect and analyze the cause of an alert. ● Contain, extradition, and recovery: Handle an alert. ● Post Incident Activity: Follow-up activities.
	Description	Alert description. The value can contain: <ul style="list-style-type: none"> ● Only uppercase letters, lowercase letters, digits, and the special characters: -_ () ● A maximum of 1,024 characters.

Step 6 Click **OK**.

----End

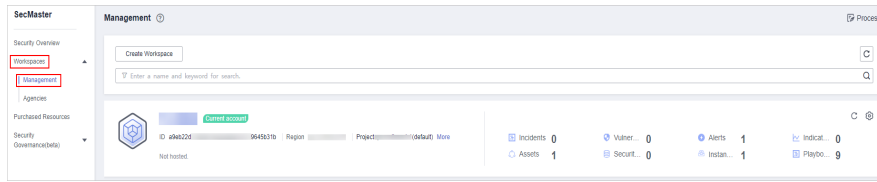
Editing an Alert

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

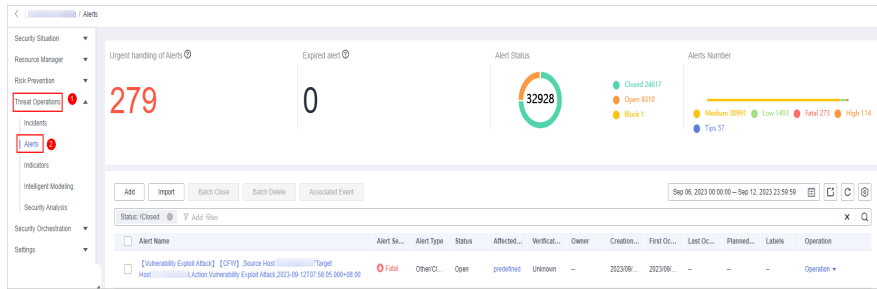
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-24 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Alerts**.

Figure 10-25 Alerts



Step 5 In the alert list, locate the row that contains the target alert, click **Edit** in the **Operation** column.

Step 6 On the **Edit** slide-out that is displayed, modify alert parameters. For details about the parameters, see [Table 10-8](#).

Table 10-8 Alert parameters

Parameter	Description	
Basic Information	Alert Name	User-defined alert name. The value must contain: <ul style="list-style-type: none"> Only uppercase letters, lowercase letters, digits, and the special characters: - _ () A maximum of 255 characters
	Alert Type	Alert type
	Alert Severity	Alert severity. The options are Tips , Low , Medium , High , and Fatal .
	Status	Alert status. The options are Open , Blocked , and Closed .
	(Optional) Owner	Primary owner of the alert.
	Data Source Product Name	Name of the data source, which cannot be changed
Data Source Type	Type of the data source, which cannot be changed	

Parameter		Description
Timeline	First Occurrence Time	Time when an alert is generated for the first time.
	Last Occurrence Time	Last time when an alert was generated
	Planned Closure Time	Time when the alert plan is disabled.
Other	Labels	Alert labels.
	Debugging data	Whether to enable simulated debugging. This parameter cannot be modified once configured.
	Verification Status	Verification status of the alert to identify the accuracy of the incident. The options are Unknown , Positive , and False positive .
	Stage	Alert phase. <ul style="list-style-type: none"> • Preparation: Prepare resources to process alert. • Detection and analysis: Detect and analyze the cause of an alert. • Contain, extradition, and recovery: Handle an alert. • Post Incident Activity: Follow-up activities.
	Description	Alert description. The value can contain: <ul style="list-style-type: none"> • Only uppercase letters, lowercase letters, digits, and the special characters: -_ () • A maximum of 1,024 characters.

Step 7 Click **OK**.

----End

10.2.4 Importing and Exporting Alerts


This section describes how to import and export alerts.

Limitations and Constraints

Only .xlsx files no larger than 20 MB can be imported.

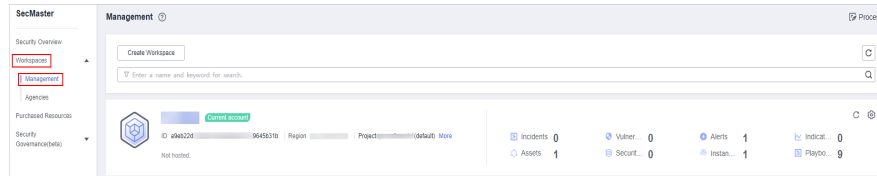
Importing Alerts

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

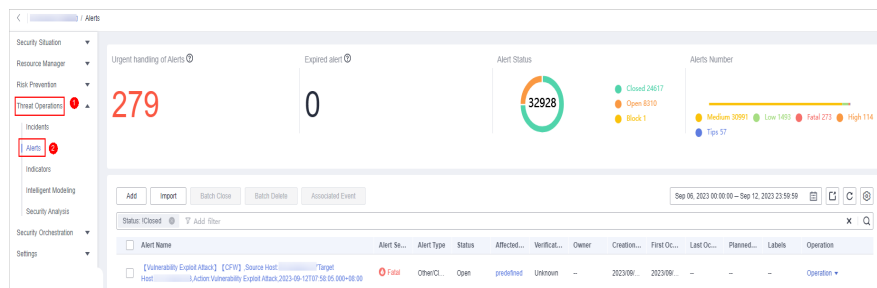
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-26 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Alerts**.

Figure 10-27 Alerts



Step 5 On the **Alerts** page, click **Import** in the upper left corner of the list.

Step 6 In the displayed **Import** dialog box, click **Download Template** to download a template, and fill in the downloaded template according to the requirements.

Step 7 After the alert file is ready, click **Select File** in the **Import** dialog box, and select the Excel file you want to import.

 **CAUTION**

- Fill in information about alerts to be imported based on the template. For details, see [Alert Template Parameters](#).
- The file must be in the .xlsx format.

Step 8 Click **OK**.

----End

Alert Template Parameters

Import alerts based on the template requirements. For details about the parameters, see [Table 10-9](#).

Table 10-9 Parameters in the alert template

Parameter	Type	Mandatory	Description
extend_properties	Object	No	Extended attribute.
ttr	Int	No	Response time.
ttd	Int	No	Detection Time.
ref_order_id	String	No	Service ID (work order ID). The value contains a maximum of 128 characters.
origin_id	String	No	Original ID of the alert. The value contains a maximum of 128 characters.
file_info	list<object>	No	File information.
user_info	list<object>	No	User information.
process	list<object>	No	Processes information.
network_list	List[Object]	No	Network information.
resource_list	List[Object]	No	Assets are affected.
system_info	object	No	System information.
alert_type	Object	Yes	Alert type. Example: <code>{"id":"demo","alert_type":"demo"}</code>
malware	Object	No	Malware.
remediation	Object	No	Remediation measures.
environment	Object	Yes	Coordinates of the environment where the alert is generated.
data_source	Object	Yes	Data source. Example: <code>{"domain_id":"demo","product_feature":"demo","project_id":"demo","product_module":"demo","company_name":"demo","region_id":"demo","source_type":-827196037,"product_name":"demo"}</code>
workspace_id	String	Yes	ID of the workspace to which the alert object belongs.
is_deleted	Boolean	No	Whether to delete the alert.


Parameter	Type	Mandatory	Description
arrive_time	Timestamp	Yes	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the alert was received. If this parameter cannot be parsed, the default time zone GMT+8 is used.
source_url	String	No	Alarm URL, which points to the page of the current incident description in the data source product.
description	String	Yes	Alert description. The value contains a maximum of 1,024 characters.
sla	Int	No	SLA for closing the incident, in hours.
ipdr_phase	String	No	Period/Phase number.
actor	String	No	Investigator
close_reason	String	No	Closure reason. <ul style="list-style-type: none"> • False detection • Resolved • Repeated • Other
close_comment	String	No	Comment for the closure.
create_time	Timestamp	Yes	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the alert was recorded. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	Timestamp	No	Closing time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the alert was disabled. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Type	Mandatory	Description
update_time	Timestamp	No	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the alert was updated. If this parameter cannot be parsed, the default time zone GMT+8 is used.
severity	String	Yes	Alert severity. The value can be: <ul style="list-style-type: none"> • Tips: No threat is found. • Low: No operation is required for the threat. • Medium: The threat needs to be handled but is not urgent. • High: The threat must be handled preferentially. • Fatal: The threat must be handled immediately to prevent further damage.
confidence	Int	No	Alert confidence. Confidence is used to illustrate the accuracy of an identified behavior or event. Value range: 0-100 <ul style="list-style-type: none"> • 0: The incident confidence is 0%. • 100: The alert confidence is 100%.
criticality	Int	No	Criticality refers to the importance level of the resources involved in an alarm. Value range: 0-100. 0 indicates that the resource is not critical, and 100 indicates that the resource is critical.
count	Int	Yes	Number of alert occurrences.
handle_status	String	Yes	Alert processing status. The value can be: <ul style="list-style-type: none"> • Open: enabled. • Block: blocked • Closed: disabled. The default value is Open .

Parameter	Type	Mandatory	Description
first_observed_time	Timestamp	Yes	First alert occurrence time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the alert was generated. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	Timestamp	No	Latest alert occurrence time, in the format of "ISO8601: YYYY-MM-DDTHH:mm:ss.ms+timezone". Time zone refers to where the alert was generated. If this parameter cannot be parsed, the default time zone GMT+8 is used.
creator	String	No	Creator.
verification_state	String	Yes	Verification status. It indicates the accuracy of an alert. The value can be: <ul style="list-style-type: none"> • Unknown: The status is unknown. • True_Positive: The status is confirmed. • False_Positive: The status is false positive. The default value is Unknown .
id	String	Yes	Unique identifier of an alert. The value is in the UUID format and contains a maximum of 36 characters.
version	String	Yes	Version of the alert object.
domain_id	String	Yes	Domain ID of the tenant to which the alert object belongs.
title	String	Yes	Alert name. The value contains a maximum of 255 characters.
region_id	String	Yes	Region ID of the tenant to which the alert object belongs.
simulation	Boolean	No	Debugging field.
owner	String	No	Owner and service owner.
labels	String	No	Labels.

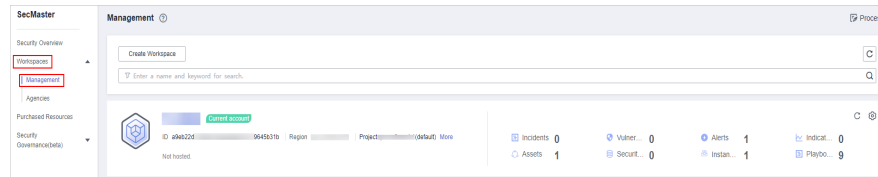
Exporting Alerts

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

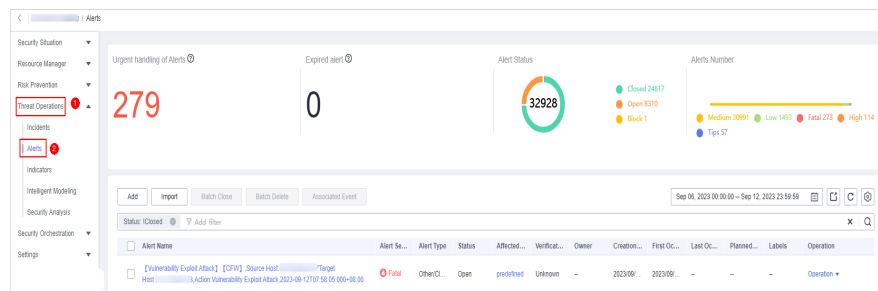
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.


Figure 10-28 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Alerts**.

Figure 10-29 Alerts



Step 5 In the alert list, select the alerts you want to export and click  in the upper right corner of the list.

Step 6 In the **Export** dialog box, set parameters.

Table 10-10 Exporting alerts

Parameter	Description
Format	By default, the alert list is exported into an Excel.
Columns	Select the indicator parameters to be exported.

Step 7 Click **OK**.

The system automatically downloads the Excel to your local PC.

----End

10.2.5 Closing or Deleting an Alert

This section describes how to perform the following operations: [Closing an Alert](#) and [Deleting an Alert](#).

Closing an Alert


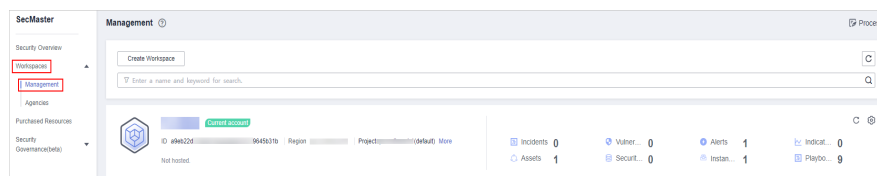
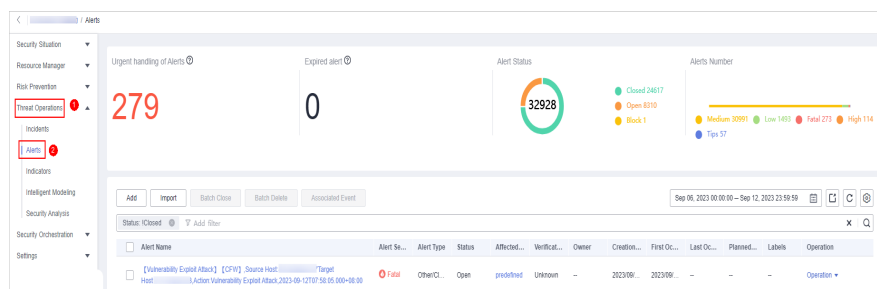
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-30 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Alerts**.

Figure 10-31 Alerts



- Step 5** In the alert list, locate the row that contains the target alert, click **More** in the **Operation** column, and select **Close**. The dialog box is displayed for you to confirm the close operation.
 - Step 6** In the confirmation dialog box, select **Reason for**, enter **Close Comment**, and click **OK**.
- End

Deleting an Alert


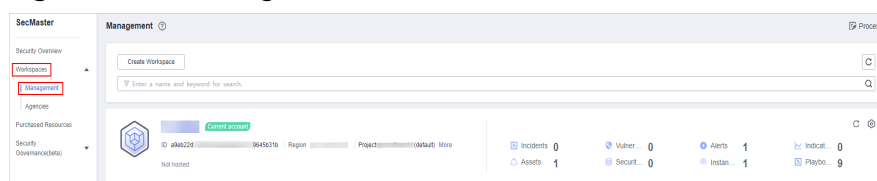
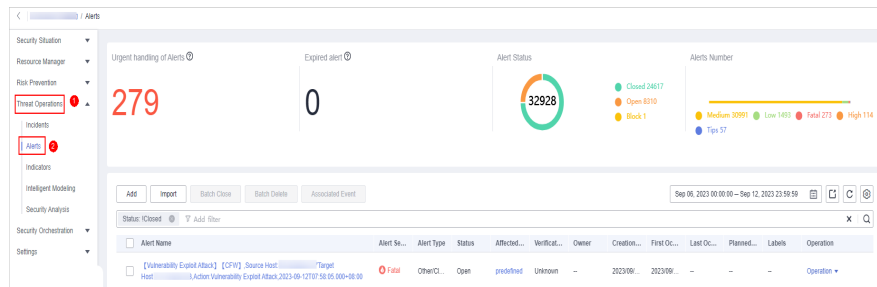
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-32 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Alerts**.

Figure 10-33 Alerts



Step 5 In the alert list, locate the row that contains the target alert, click **More** in the **Operation** column, and select **Delete**. The deletion confirmation dialog box is displayed.

Step 6 In the displayed dialog box, click **OK**.

NOTE

Deleted alerts cannot be retrieved. Exercise caution when performing this operation.

----End

10.3 Indicator Management

10.3.1 Creating an Indicator

The indicator library list displays information about all your indicators.

This section describes how to create an indicator.

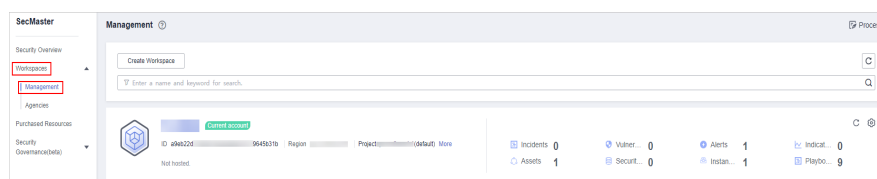
Procedure

Step 1 Log in to the management console.

Step 2 Click **☰** in the upper left corner of the page and choose **Security > SecMaster**.

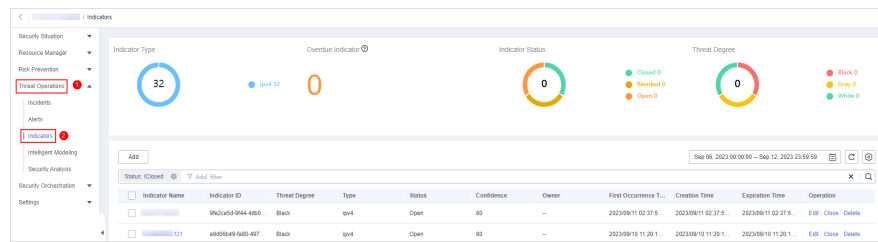
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-34 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Indicators**.

Figure 10-35 Indicators



Step 5 On the **Indicators** page, click **Add**. On the **Add** page, set parameters.

Table 10-11 Indicator parameters

Parameter	Description
Indicator Name	Name of a user-defined threat indicator. The value can contain: Only uppercase letters, lowercase letters, digits, and the special characters: -_ ()
Type	Indicator type.
Threat Degree	Select a threat degree level. <ul style="list-style-type: none"> ● Black: dangerous ● Gray: minor ● White: secure
Data Source Product Name	Data source product name
Data Source Type	Type of the data source.
Status	Indicator status. Possible values are Open , Closed , and Revoked .
(Optional) Confidence	Reliability of the selected indicator. The value ranges from 80 to 100.
(Optional) Owner	Primary owner of the indicator.
(Optional) Labels	Label of a user-defined counter.
First Occurrence Time	First occurrence time of the indicator.
Last Occurrence Time	Latest occurrence time of the indicator.
(Optional) Expiration Time	Expiration time of the indicator.
Invalid or not	Whether to invalidate the indicator. The default value is No .

Parameter	Description
Granularity	Granularity of the indicator. The options are First time observed , Self-produced data , To be purchased , and Query from external network .
<i>Other parameters</i>	You need to set the parameters based on the selected type. Set the parameters as prompted. For example, if you select ipv6 for Type , you also need to configure the IP address, email account, and region.

Step 6 Click **OK**.


----End

10.3.2 Disabling Indicators

This topic describes how to disable indicators.

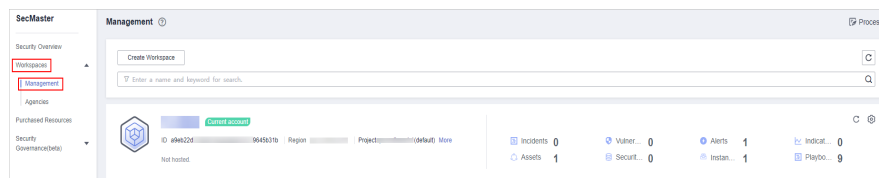
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

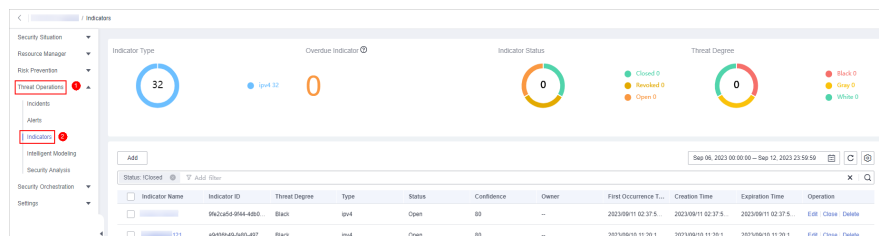
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-36 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Indicators**.

Figure 10-37 Indicators



Step 5 On the **Indicator** page, locate the row that contains the target indicator, click **Close** in the **Operation** column. The **Close** dialog box is displayed.

Step 6 In the dialog box that is displayed, select the close reason and enter comments.

Step 7 Click **OK**.

----End

10.3.3 Importing and Exporting Intelligence Indicators


This section describes how to import intelligence indicators.

Constraints

- Only .xlsx files no larger than 20 MB can be imported.
- A maximum of 9,999 indicator records can be exported.

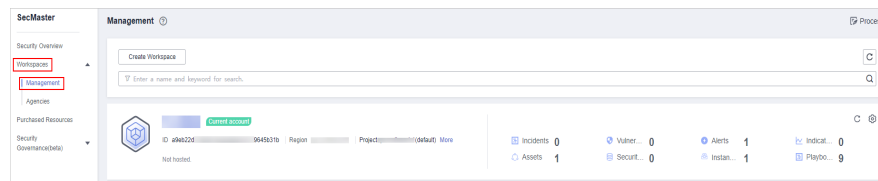
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

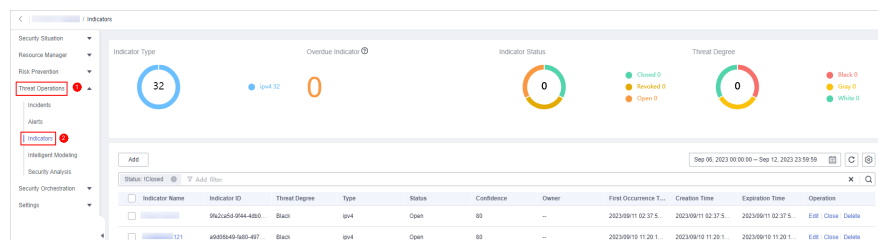
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-38 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Indicators**.

Figure 10-39 Indicators



Step 5 On the **Indicator** page, click **Import** in the upper left corner above the indicator list.

Step 6 In the displayed **Import** dialog box, click **Download Template** to download a template, and fill in the downloaded template according to the requirements.

Step 7 After the indicator file is ready, click **Select File** in the **Import** dialog box, and select the Excel file you want to import.

 **CAUTION**

- Fill in information about the intelligence indicators to be imported based on the template. For details, see [Parameters in the Intelligence Indicator Template](#).
- The file must be in the .xlsx format.

Step 8 Click **OK**.

----End

Parameters in the Intelligence Indicator Template

Import intelligence indicators based on the template requirements. For details about the parameters, see [Table 10-12](#).

Table 10-12 Parameters in the intelligence indicator template

Parameter	Type	Mandato ry	Description
data_source	Object	Yes	Data source. Example: { "domain_id": "demo", "product_feature": "demo", "project_id": "demo", "product_module": "demo", "company_name": "demo", "region_id": "demo", "source_type": "892339122", "product_name": "demo" }
environment	Object	Yes	Coordinates of the environment where the indicator is generated. Example: { "domain_id": "demo", "project_id": "demo", "region_id": "demo", "vendor_type": "demo" }
email	Object	No	Email.
url	Object	No	URL.
domain	Object	No	Domain name.
is_deleted	string	Yes	Whether to delete the indicator.
workspace_id	String	Yes	Workspace ID.
weak_password	String	No	Weak password.
vulnerability	String	No	Vulnerability.
start_time	Timestamp	No	Start time.
information_source	String	Yes	Source.
confidence	Numeric	No	Indicator confidence. Its value range is 80 to 100.

Parameter	Type	Mandatory	Description
close_comment	String	No	Comment for the closure.
labels	String	No	Labels, such as mine pool and outreach .
inactive_time	Timestamp	No	Expiration time.
file	Object	No	File.
close_reason	String	No	Closure reason.
first_report_time	Timestamp	Yes	First occurrence time.
create_time	Timestamp	Yes	Creation time of the intelligence collected by the threat platform.
suggested_of_coa	String	No	Suggestion.
valid_from	Timestamp	No	Start time of the validity period, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the indicator validity period started. If this parameter cannot be parsed, the default time zone GMT+8 is used.
kill_chain_phases	String	No	Important information that should be retained.
verdict	String	Yes	Threat degree indicated by colors black, white, and gray.
pattern	String	No	Reserved field.
external_references	String	No	Extended field.
status	String	Yes	Indicator status. The value can be: <ul style="list-style-type: none"> • Open: enabled. • Closed: disabled. • Revoked: invalid.
revoked	Boolean	No	Whether the indicator is revoked. The default value is No .
creator	String	No	Creator.

Parameter	Type	Mandatory	Description
granular_marking	Numeric	Yes	Granularity (confidentiality level). The value can be 1 (first discovery), 2 (self-produced data), 3 (purchase required), and 4 (direct query from the external network) in descending order.
id	String	Yes	Unique ID, which is generated according to the following rule: MD5 (indicator_type + value + information_source + label)
owner	String	No	Owner.
ip	Object	No	IP address.
indicator_type	Object	Yes	Indicator type. The value can be ipv4 , ipv6 , domain , email , url , hash , and un_classified . Example: <pre>{"indicator_type":"demo","id":"demo","category":"demo"}</pre>
close_time	String	No	Closing time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the indicator occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
inactive_set_time	Timestamp	No	Expiration time.
update_time	String	No	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the indicator was updated. If this parameter cannot be parsed, the default time zone GMT+8 is used.
verdict_set_time	Timestamp	No	Verdict time.
severity	Numeric	No	Severity. The value varies depending on the channel. The value ranges from 80 to 100.

Parameter	Type	Mandatory	Description
valid_until	Timestamp	No	End time of the validity period, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the indicator validity period ended. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_report_time	Timestamp	Yes	Latest occurrence time.
value	String	Yes	Value, such as ip , url , and domain .
defanged	Boolean	Yes	Whether the indicator is invalid. The default value is No .
extensions	String	No	Extensions.
count	Numeric	No	Occurrences.
description	String	No	Description
name	String	Yes	Intelligence name.

Exporting Indicators


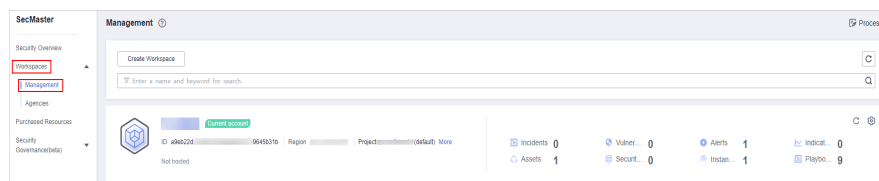
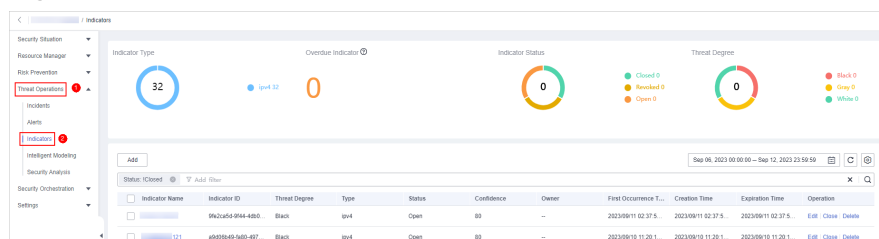
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.


Figure 10-40 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Indicators**.

Figure 10-41 Indicators



Step 5 On the **Indicators** page, select the indicators you want to export and click  in the upper right corner of the list. The **Export** dialog box is displayed.

Step 6 In the **Export** dialog box, set parameters.

Table 10-13 Exporting indicators

Parameter	Description
Format	By default, the indicator list is exported into an Excel.
Columns	Select the indicator parameters to be exported.

Step 7 Click **OK**.

The system automatically downloads the Excel to your local PC.


----End

10.3.4 Managing Indicators

This section describes how to perform operations such as [Viewing an Indicator](#), [Editing an Indicator](#), and [Deleting an Indicator](#).

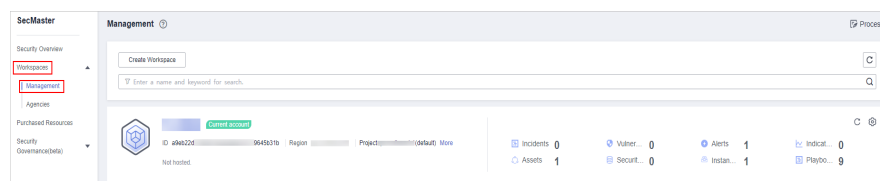
Viewing an Indicator

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

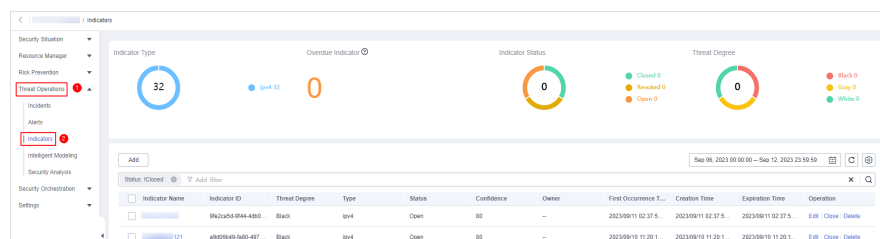
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-42 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Indicators**.

Figure 10-43 Indicators



Step 5 In the upper part of the **Indicators** page, view threat indicator statistics.

Figure 10-44 Indicator overview



- **Indicator Type:** displays the total number of indicators of all types and the number of indicators of the corresponding type.
- **Overdue Indicator:** displays the total number of threat indicators that have expired and have not been closed.
- **Indicator Status:** displays the total number of indicators in different states and the number of indicators in the corresponding state.
- **Threat Degree:** displays the number of indicators corresponding to different threat levels.

Step 6 In the indicator management list, view the indicator details. For details about the parameters, see [Table 10-14](#).

You can view a maximum of 9,999 indicator records on the page.

Table 10-14 Indicator parameters

Parameter	Description
Indicator Name	Indicator name.
Indicator ID	ID of an indicator.
Threat Degree	Threat degree corresponding to an indicator. The options are black, white, and gray.
Type	Indicator type.
Status	Indicator status. The options are Open , Closed , and Revoked .
Confidence	Confidence of an indicator.
Owner	Owner of an indicator.
First Occurrence Time	First occurrence time of the indicator.
Creation Time	Time when an indicator was created.
Expiration Time	Time when an indicator expires.
Operation	Operations that can be performed for an indicator, including editing, closing, and deleting an indicator.

Step 7 To view details about an indicator, click the indicator name. The indicator details are displayed on the right of the page.

----End

Editing an Indicator


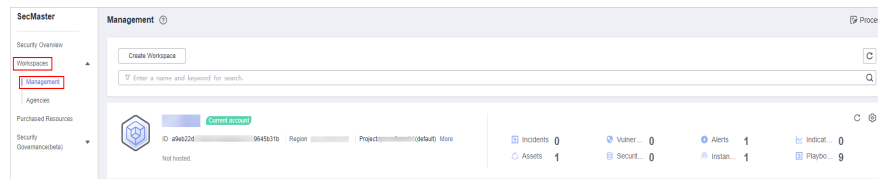
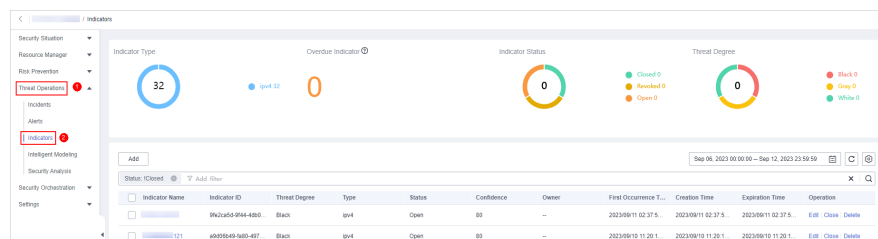
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-45 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Indicators**.

Figure 10-46 Indicators



- Step 5** On the **Indicators** page, locate the target indicator and click **Edit** in the **Operation** column.
- Step 6** On the **Edit** page that is displayed, edit indicator parameters.

Table 10-15 Indicator parameters

Parameter	Description
Indicator Name	Name of a user-defined threat indicator. The value can contain: Only letters, digits, and special characters (-_()).
Type	Indicator type
Threat Degree	Select a threat level. <ul style="list-style-type: none"> ● Black: dangerous ● Gray: minor ● White: secure
Data Source Product Name	Name of the data source, which cannot be changed
Data Source Type	Type of the data source, which cannot be changed


Parameter	Description
Status	Indicator status. Possible values are Open , Closed , and Revoked .
Confidence	Reliability of the selected indicator. The value ranges from 80 to 100.
Owner	Primary owner of the indicator.
Labels	Label of a user-defined indicator.
First Occurrence Time	First occurrence time of the indicator.
Last Occurrence Time	Latest occurrence time of the indicator.
Expiration Time	Expiration time of the indicator.
Invalid or not	Whether to invalidate the indicator. The default value is No .
Granularity	Granularity of the indicator. The options are First time observed , Self-produced data , To be purchased , and Query from external network .
<i>Other parameters</i>	You need to set the parameters based on the selected type. For example, if you select ipv6 for Type , you also need to configure the IP address, email account, and region.

Step 7 Click **OK**.

----End

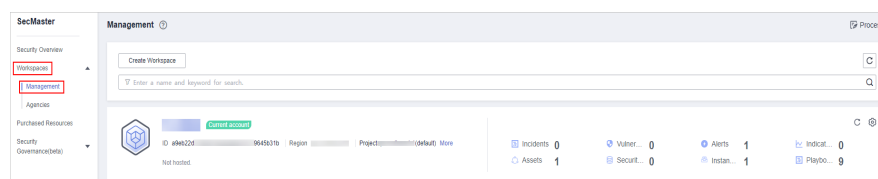
Deleting an Indicator

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

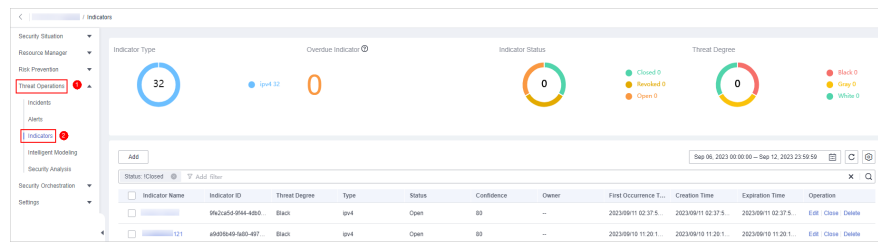
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-47 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Indicators**.

Figure 10-48 Indicators



Step 5 On the **Indicators** page, locate the target indicator and click **Delete** in the **Operation** column.

Step 6 In the dialog box that is displayed, click **OK**.

NOTE

Deleted indicators cannot be restored. Exercise caution when performing this operation.

----End

10.4 Intelligent Modeling


10.4.1 Viewing Existing Model Templates

SecMaster uses models to scan log data in pipes. If the data is not within the model range, an alert is generated. Models are created based on templates. Therefore, you need to use existing templates to create models.

This section describes how to view existing model templates.

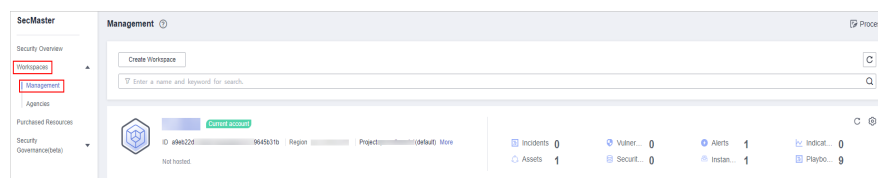
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

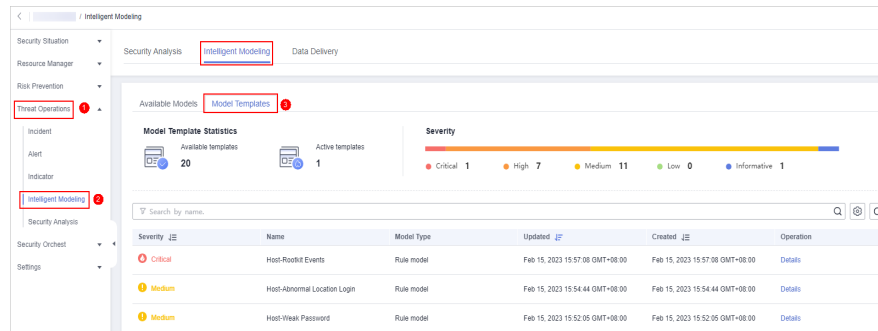
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-49 Management



Step 4 In the navigation tree on the left, choose **Threat Operations > Intelligent Modeling**. On the Intelligent Modeling page that is displayed, click the **Model Templates** tab. The Model Template page is displayed.

Figure 10-50 Model Templates tab page



Step 5 On the **Model Templates** page, view existing model templates.

- **Model Template Statistics:** Displays the number of **available templates** and the number of **active templates**.
- **Severity:** displays the severity statistics of existing templates, including critical, high-risk, medium-risk, low-risk, and warning.
- The template list displays the severity, name, model type, update time, and creation time of the existing templates.
- To view details about a model template, locate the row that contains the template, click **Details** in the **Operation** column. The template details page is displayed on the right.

On the details page, you can view the description, query rules, triggering conditions, and query plans of the current model template.

----End

10.4.2 Creating/Editing a Model


SecMaster can use models to monitor log data in pipelines. If the data is not within the model scope, an alert is generated.

This topic describes how to create and edit an alert model.

- [Creating an Alarm Model Using an Existing Template](#)
- [Customizing an Alert Model](#)
- [Editing a Model](#)

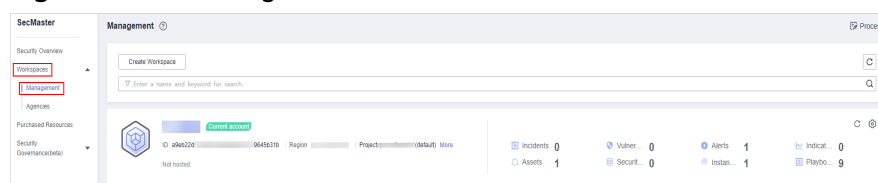
Creating an Alarm Model Using an Existing Template

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

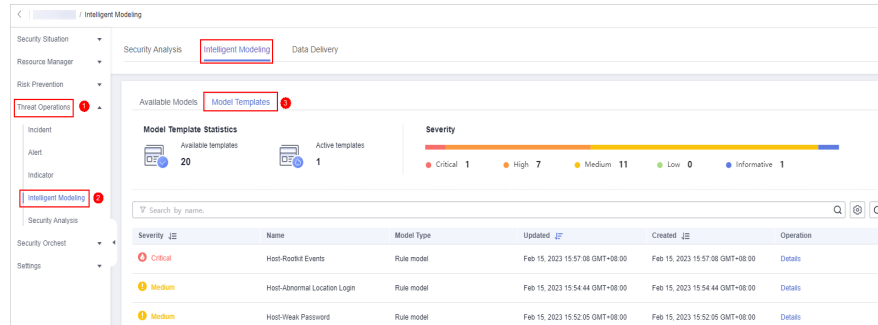
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-51 Management



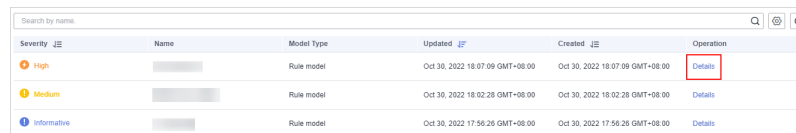
Step 4 In the navigation tree on the left, choose **Threat Operations > Intelligent Modeling**. On the Intelligent Modeling page that is displayed, click the **Model Templates** tab. The Model Template page is displayed.

Figure 10-52 Model Templates tab page



Step 5 In the model template list, click **Details** in the **Operation** column of the target model template. The template details page is displayed on the right.

Figure 10-53 Model template details



Step 6 On the model template details page, click **Create Model** in the lower right corner. The page for creating an alert model is displayed.

Step 7 On the Add Alarm Model page, configure basic information about the alert model. For details about the parameters, see [Table 10-16](#).

Figure 10-54 Basic configuration

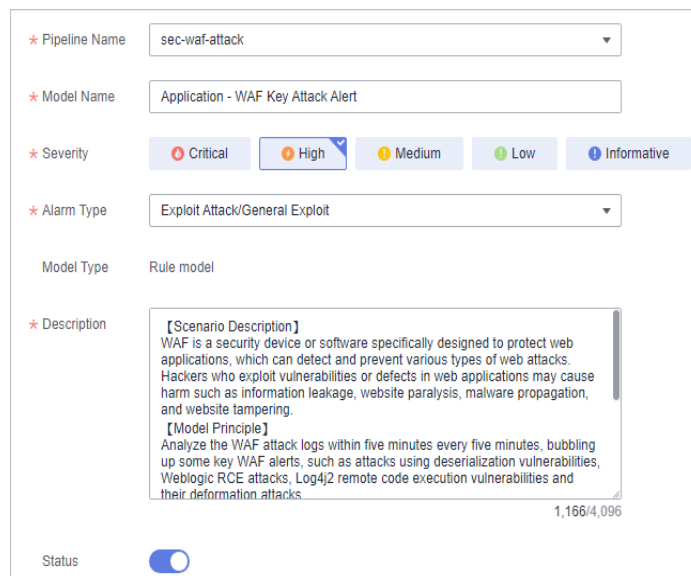




Table 10-16 Basic alert model parameters



Parameter	Description
Pipeline Name	Select the execution pipeline of the alert model.
Model Name	Name of the alert model.
Severity	Severity of the alert model. You can set the severity to Critical, High, Medium Low, or Informative.
Alarm Type	Alarm type displayed after the alert model is triggered.
Model Type	The default value is Rule model.
Description	Description of the alert model
Status	<p>Indicates whether to enable the alert model.</p> <ul style="list-style-type: none">  : indicates that the model is enabled. This is the default status.  : indicates that the model is disabled. <p>The status set here can be changed after the entire alert model is set successfully.</p>

Step 8 After the setting is complete, click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.

Step 9 Set the model logic. For details about the parameters, see [Table 10-17](#).

Table 10-17 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click Run and view the running result.

Parameter	Description
Query Plan	<p>Set an alert query plan.</p> <ul style="list-style-type: none"> Running query interval: xx minutes/hour/day. If the running query interval is minute, set this parameter to a value ranging from 5 to 59 minutes. If the running query interval is hour, set this parameter to a value ranging from 1 to 23 hours. If the running query interval is day, set this parameter to a value ranging from 1 to 14 days. Time window: xx minutes/hour/day. If the time window is minute, the value ranges from 5 minutes to 59 minutes. If the time window is hour, the value ranges from 1 hour to 23 hours. If the time window is day, the value ranges from 1 day to 14 days. Execution Delay: xx minutes. The value ranges from 0 to 5 minutes.
Advanced Alarm Settings	<ul style="list-style-type: none"> Custom Information: Customize extended alert information. Click Add, and set the key and value information. Alarm Details: Enter the alarm name, description, and handling suggestions.
Trigger Condition	<p>Sets alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx.</p> <p>If there are multiple triggers, click Add.</p>
Alarm Trigger	<p>The way to trigger alerts for queried results. The options are as follows:</p> <ul style="list-style-type: none"> One alert for all query results One alert for each query result
Debugging	<p>Sets whether to generate debugging alarms.</p>
Suppression	<p>Specifies whether to stop the query after an alert is generated.</p> <ul style="list-style-type: none">  : indicates that the query stops after an alert is generated.  : indicates that the query is not stopped after an alert is generated.


Step 10 After the setting is complete, click **Next** in the lower right corner of the page. The model details preview page is displayed.

Step 11 After confirming that the preview is correct, click **OK** in the lower right corner of the page.

----End

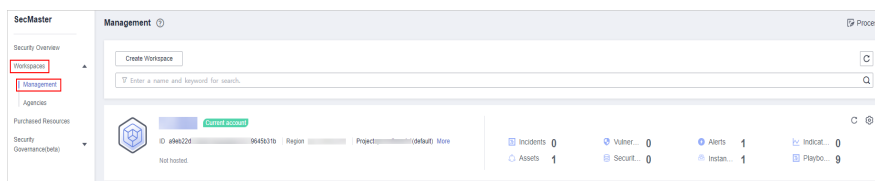
Customizing an Alert Model

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

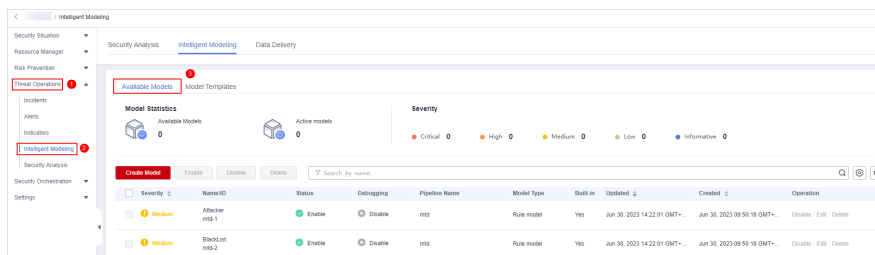
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-55 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Intelligent Modeling**.

Figure 10-56 Available Models





Step 5 Click **Create Model** in the upper left corner of the **Available Models** tab.

Step 6 On the **Create Model** slide-out panel displayed, configure basic information about the alert model. For details about the parameters, see [Table 10-18](#).

Figure 10-57 Basic configuration



Table 10-18 Basic alert model parameters

Parameter	Description
Pipeline Name	Select the execution pipeline of the alert model.
Model Name	Name of the alert model.
Severity	Severity of the alert model. You can set the severity to Critical, High Risk, Medium Risk, Low Risk, or Warning.
Alarm Type	Alarm type displayed after the alert model is triggered.
Model Type	The default value is Rule model .
Description	Description of the alert model
Status	<p>Indicates whether to enable the alert model.</p> <ul style="list-style-type: none">  : indicates that the model is enabled. This is the default status.  : indicates that the model is disabled. <p>The status set here can be changed after the entire alert model is set successfully.</p>

Step 7 After the setting is complete, click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.

Step 8 Set the model logic. For details about the parameters, see [Table 10-19](#).

Table 10-19 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click Run and view the running result. For details about the syntax, see SQL Syntax .
Query Plan	Set an alert query plan. <ul style="list-style-type: none"> Running query interval: xx minutes/hour/day. If the running query interval is minute, set this parameter to a value ranging from 5 to 59 minutes. If the running query interval is hour, set this parameter to a value ranging from 1 to 23 hours. If the running query interval is day, set this parameter to a value ranging from 1 to 14 days. Time window: xx minutes/hour/day. If the time window is minute, the value ranges from 5 minutes to 59 minutes. If the time window is hour, the value ranges from 1 hour to 23 hours. If the time window is day, the value ranges from 1 day to 14 days. Execution Delay: xx minutes. The value ranges from 0 to 5 minutes.
Advanced Alarm Settings	<ul style="list-style-type: none"> Extended information about a user-defined alert. Click Add, and set the Key and Value information. Alarm Details: Enter the alarm name, description, and handling suggestions.
Trigger Condition	Setting alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx.
Alarm Trigger	The way to trigger alerts for queried result. The options are as follows: <ul style="list-style-type: none"> One alert for all query results One alert for each query result
Debugging	Sets whether to generate debugging alarms.
Suppression	Specifies whether to stop the query after an alert is generated. <ul style="list-style-type: none"> : indicates that the query stops after an alert is generated. : indicates that the query is not stopped after an alert is generated.

Step 9 After the setting is complete, click **Next** in the lower right corner of the page. The model details preview page is displayed.


Step 10 After confirming that the preview is correct, click **OK** in the lower right corner of the page.

----End

Editing a Model

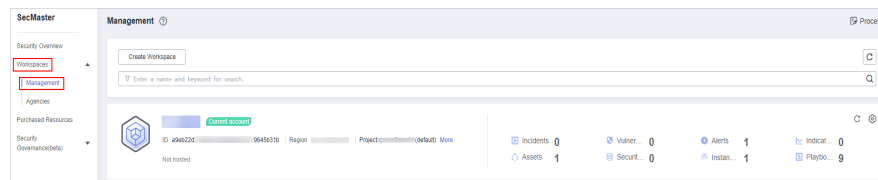
Only custom models can be edited.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

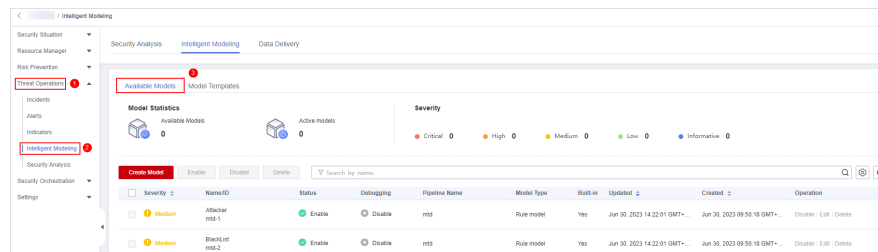
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-58 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Intelligent Modeling**.

Figure 10-59 Available Models



Step 5 In the available model list, click **Edit** in the **Operation** column of the target model.

Step 6 On the **Edit Model** slide-out panel, configure basic information about the alert model. For details about the parameters, see [Table 10-20](#).

Figure 10-60 Basic configuration

The screenshot shows a configuration form with the following fields and values:

- Pipeline Name:** sec-waf-attack
- Model Name:** Application - WAF Key Attack Alert
- Severity:** High (selected from Critical, High, Medium, Low, Informative)
- Alarm Type:** Exploit Attack/General Exploit
- Model Type:** Rule model
- Description:**
 - Scenario Description:** WAF is a security device or software specifically designed to protect web applications, which can detect and prevent various types of web attacks. Hackers who exploit vulnerabilities or defects in web applications may cause harm such as information leakage, website paralysis, malware propagation, and website tampering.
 - Model Principle:** Analyze the WAF attack logs within five minutes every five minutes, bubbling up some key WAF alerts, such as attacks using deserialization vulnerabilities, Weblogic RCE attacks, Log4j2 remote code execution vulnerabilities and their deformation attacks.
- Status:** Enabled (toggle switch)

Table 10-20 Basic alert model parameters



Parameter	Description
Pipeline Name	Select the execution pipeline of the alert model. Editing the pipeline name is not supported currently.
Model Name	Name of the alert model.
Severity	Severity of the alert model. You can set the severity to Critical , High , Medium , Low , or Informative .
Alarm Type	Alarm type displayed after the alert model is triggered.
Model Type	The default value is Rule model .
Description	Description of the alert model

Step 7 After the setting is complete, click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.

Step 8 Set the model logic. For details about the parameters, see [Table 10-21](#).

Table 10-21 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click Run and view the running result.

Parameter	Description
Query Plan	<p>Set an alert query plan.</p> <ul style="list-style-type: none"> Running query interval: xx minutes/hour/day. If the running query interval is minute, set this parameter to a value ranging from 5 to 59 minutes. If the running query interval is hour, set this parameter to a value ranging from 1 to 23 hours. If the running query interval is day, set this parameter to a value ranging from 1 to 14 days. Time window: xx minutes/hour/day. If the time window is minute, the value ranges from 5 minutes to 59 minutes. If the time window is hour, the value ranges from 1 hour to 23 hours. If the time window is day, the value ranges from 1 day to 14 days. Execution Delay: xx minutes. The value ranges from 0 to 5 minutes.
Advanced Alarm Settings	<ul style="list-style-type: none"> Custom Information: Customize extended alert information. Click Add, and set the key and value information. Alarm Details: Enter the alarm name, description, and handling suggestions.
Trigger Condition	<p>Sets alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx.</p> <p>If there are multiple triggers, click Add.</p>
Alarm Trigger	<p>The way to trigger alerts for queried results. The options are as follows:</p> <ul style="list-style-type: none"> One alert for all query results One alert for each query result
Debugging	<p>Sets whether to generate debugging alarms.</p>
Suppression	<p>Specifies whether to stop the query after an alert is generated.</p> <ul style="list-style-type: none">  : indicates that the query stops after an alert is generated.  : indicates that the query is not stopped after an alert is generated.

Step 9 After the setting is complete, click **Next** in the lower right corner of the page. The model details preview page is displayed.

Step 10 After confirming that the preview is correct, click **OK** in the lower right corner of the page.

----End

10.4.3 Viewing Existing Models


This topic describes how to view existing models.

Prerequisites

A model has been created. For details, see [Creating/Editing a Model](#).

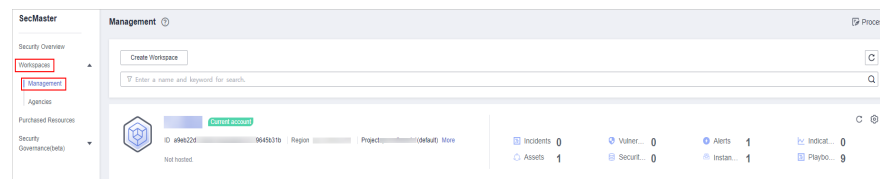
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

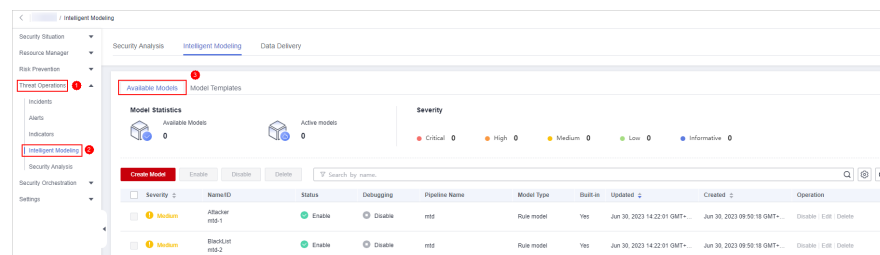
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-61 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Intelligent Modeling**.

Figure 10-62 Available Models



Step 5 On the **Available Models** tab, view existing models.

- **Model Statistics:** displays the number of available models and the number of active models.
- **Severity:** displays the severity statistics of existing models. The options are **Critical, High, Medium, Low, and Informative**.
- The model list displays the severity, name/ID, pipe name, model type, update time, and creation time of existing models.

----End

10.4.4 Managing Models


This topic walks you through how to manage models, such as enabling, disabling, and deleting a model.

Limitations and Constraints

- Only custom models can be enabled, disabled, and deleted.

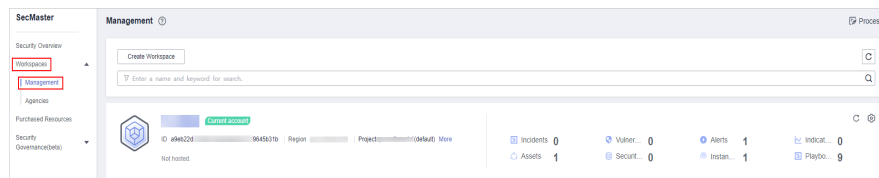
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

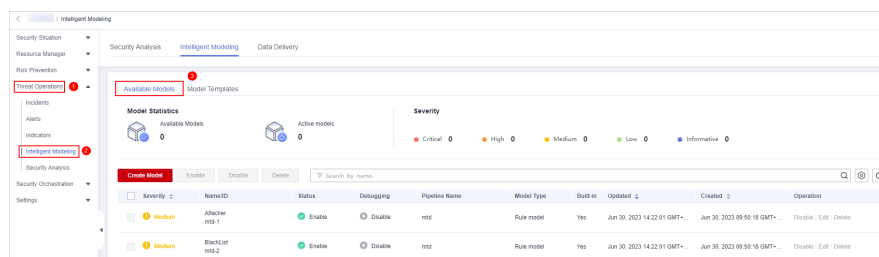
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-63 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Intelligent Modeling**.

Figure 10-64 Available Models



Step 5 Manage models.

Table 10-22 Managing models

Parameter	Description
Enable	<p>In the model list, click Enable in the Operation column of the target model.</p> <p>NOTE</p> <p>To enable models in batches, select all models you want to start and click Enable in the upper left corner of the list.</p> <p>If the model status changes to Enable, the model is successfully started.</p>

Parameter	Description
Disable	<p>In the model list, locate the row that contains the target model and click Disable in the Operation column.</p> <p>NOTE To disable models in batches, select all models and click Disable in the upper left corner of the list.</p> <p>When the alert model status changes to Disable, the model is disabled.</p>
Delete	<p>1. In the model list, locate the row that contains the target model and click Delete in the Operation column.</p> <p>NOTE To delete models in batches, select all models to be deleted and click Delete in the upper left corner of the list.</p> <p>2. In the displayed dialog box, click OK.</p>

----End

10.5 Security Analysis

10.5.1 Security Analysis Overview

The security analysis function works as a cloud native security information and event management (SIEM) solution in SecMaster. It can collect, aggregate, and analyze security logs and alarms from multiple products and sources based on predefined and user-defined threat detection rules. It helps quickly detect and respond to security incidents and protect cloud workloads, applications, and data.

Limitations and Constraints

- A maximum of 500 results can be returned for a single analysis query.
- A maximum of 50 shortcut queries can be created in a pipeline. That is, a maximum of 50 query analysis criteria can be saved as shortcut queries.
- A maximum of 5 data spaces can be created in a workspace, and a maximum of 20 pipelines can be created in a data space.
- A maximum of 64 shards can be allocated to a pipeline.
- The maximum data retention period in a pipeline is 180 days.

10.5.2 Getting Started

[Table 10-23](#) shows the process of using the security analysis function.

Table 10-23 Process

Step	Description
Adding a Workspace	Add a workspace for resource isolation and control.
Integrating Data	Configure the data to be accessed. SecMaster can integrate log data of multiple products, such as storage, management and supervision, and security. After the integration, you can search for and analyze all collected logs.
(Optional) Adding a Data Space	Create a data space for storing collected log data. For data accessed through the console, the system creates a default data space. You do not need to create a data space.
(Optional) Creating a Pipeline	Create pipelines for collecting, storing, and querying log data. For data accessed through the console, the system creates a default data pipeline. You do not need to create a pipeline.
Configuring Indexes	Configure indexes to narrow down the query scope.
Querying and Analyzing Data	Query and analyze the accessed data.
Downloading Logs	Allows you to download raw logs or queried and analyzed logs.
Querying Analysis Results in Charts and Tables	After you run query and analysis statements, SecMaster can display the query and analysis results in charts and tables. Currently, data can be displayed in tables, line charts, bar charts, and pie charts.

10.5.3 Configuring Indexes

An index in security analysis is a storage structure used to sort one or more columns in log data. Different index configurations generate different query and analysis results. Configure indexes based on your requirements.

If you want to use the analysis function, you must configure field indexes. After configuring a field index, you can specify field keys and field values to narrow down the query scope. For example, the query statement **level:error** is to query logs whose **level** field contains the value **error**.

Prerequisites

Data access has been completed. For details, see [Data Integration](#).

Configuring Field Indexes


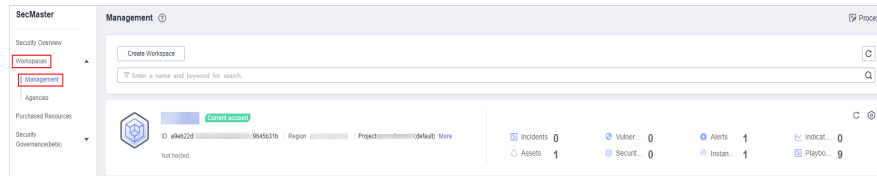
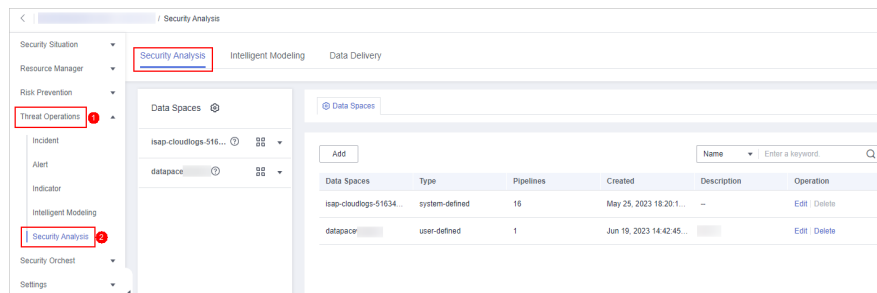
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-65 Management



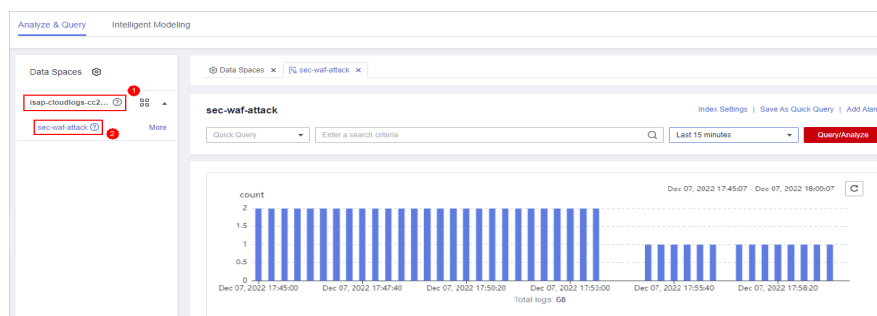
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-66 Accessing the Security Analysis tab page



- Step 5** In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-67 Pipeline data page



- Step 6** On the pipeline page, click **Index Settings** in the upper right corner.
- Step 7** On the **Index Settings** page, configure index parameters.
 1. Enable the index status.

The index status is enabled by default. When the index status is disabled, collected logs cannot be queried using indexes.

2. Configure index parameters. For details about the parameters, see [Table 10-24](#).

Figure 10-68 Index Settings

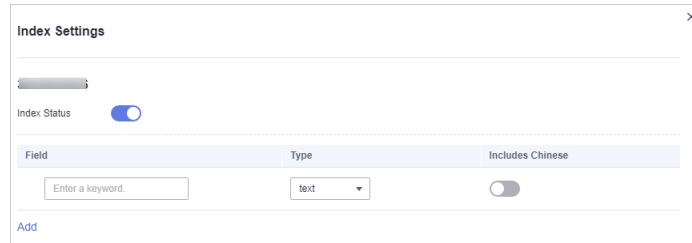


Table 10-24 Parameters for index settings

Parameter	Description
Field	Log field (key)
Type	Data type of the log field value. The options are text, keyword, long, integer, double, float, date, and json.
Includes Chinese	<p>Indicates whether to distinguish between Chinese and English during query. This parameter needs to be specified when Type is set to text.</p> <ul style="list-style-type: none"> – After the function is enabled, if the log contains Chinese characters, the Chinese content is split based on the Chinese grammar and the English content is split based on delimiters. – After this function is disabled, all content is split based on delimiters. <p>Example: The log content is user:WAF log user Zhang San.</p> <ul style="list-style-type: none"> – After Includes Chinese is disabled, the log is split based on the colon (:). So it is split into user and WAF log user Zhang San. You can search for the log by user or WAF log user Mr. Zhang. – After Includes Chinese is enabled, the LTS background analyzer splits the log into user, WAF, log, user, and Zhang San. You can find logs by searching for log or Mr. Zhang.

Step 8 Click **OK**.

----End

10.5.4 Querying and Analyzing Data

You can query and analyze collected log data in real time on the **Analyze & Query** tab.

This topic walks you through how to query and analyze log data.


- [Entering Query Criteria for Query and Analysis](#)
- [Using Existing Fields for Query and Analysis](#)
- [Managing Query Analysis Results](#)

Prerequisites

Data access has been completed. For details, see [Data Integration](#).

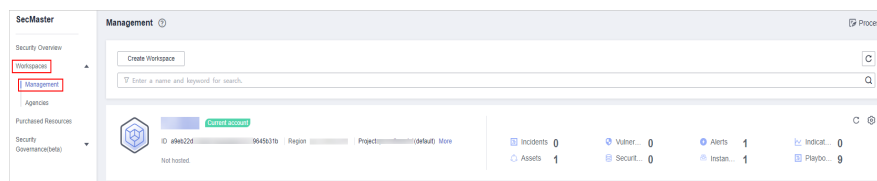
Entering Query Criteria for Query and Analysis

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

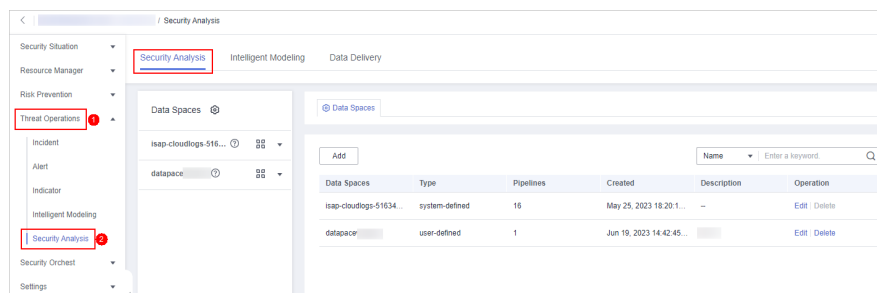
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-69 Management



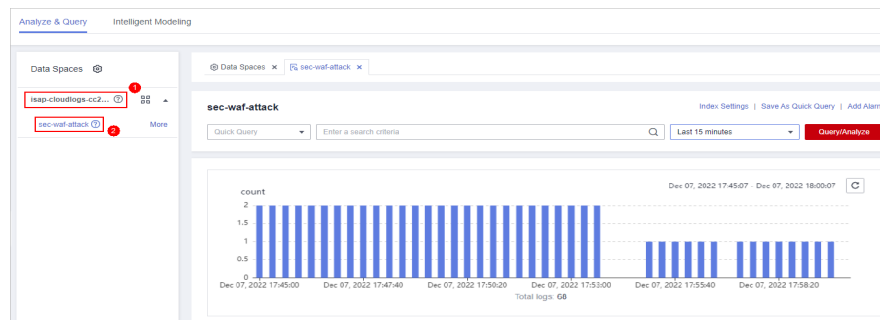
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-70 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-71 Pipeline data page



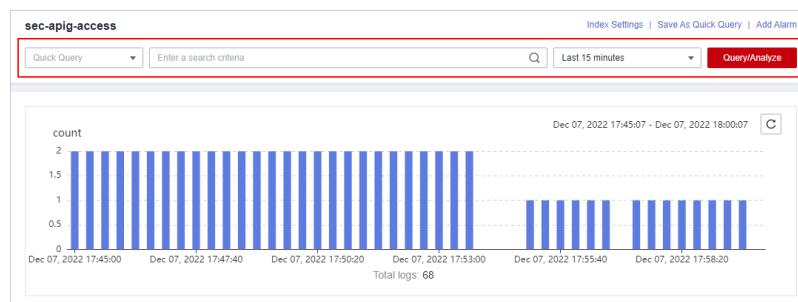
Step 6 On the pipeline data retrieval page, enter the query analysis statement.

A query analysis statement consists of a query statement and an analysis statement. The format is **Query Statement|Analysis Statement**. For details about the syntax of query analysis statements, see [Query and Analysis Syntax](#).

NOTE

If the reserved field is of the text type, **MATCH_QUERY** is used for word segmentation query by default.

Figure 10-72 Query/Analyze



Step 7 Select **Last 15 minutes** as the time range.

You can select **Last 15 minutes**, **Last hour**, or **Last 24 hours** or customize a time range for the query.


Step 8 Click **Query/Analyze** and view the results.

----End

Using Existing Fields for Query and Analysis

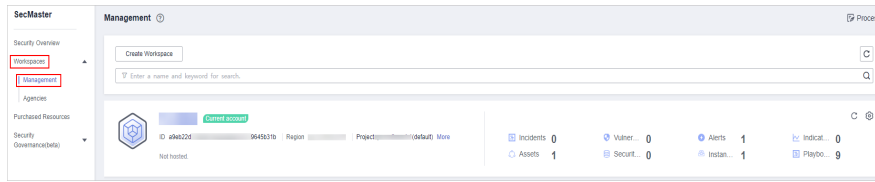
The following part describes how to use existing fields to query and analyze logs.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

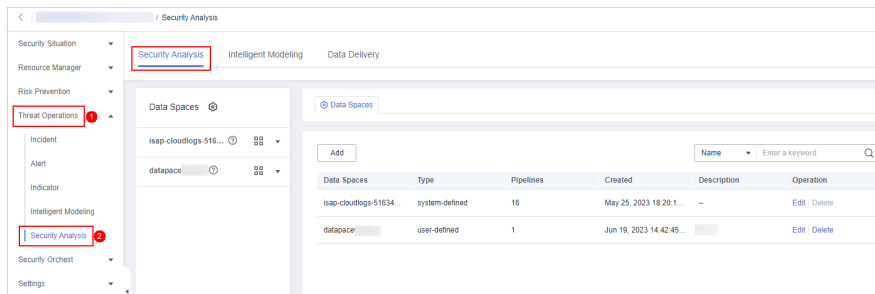
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-73 Management



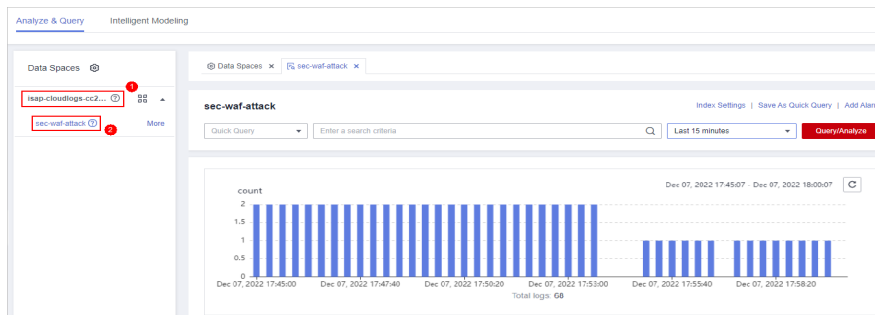
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-74 Accessing the Security Analysis tab page



Step 5 In the **Data Spaces** tree on the left, click a data space name to show the pipeline list. Then, click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-75 Pipeline data page



Step 6 Set search criteria.

NOTE

If the reserved field is of the text type, **MATCH_QUERY** is used for word segmentation query by default.

- Click \checkmark before an optional field on the left and click \oplus (adding a field value) or \ominus (removing a field value) next to the target field. The matched fields are displayed in the query box.
- If you have expanded the log data at a specific time point and need to filter some fields, click \oplus (adding a field value) or \ominus (removing a field value) in front of the field name. The query box displays the matched fields.

Step 7 By default, data in the last 15 minutes is queried and displayed. If you want to query log data in other time ranges, set the query time and click **Query/Analyze**.

----End


Managing Query Analysis Results







SecMaster displays query and analysis results in the form of log distribution bar charts, **Raw Logs**, and **Charts**.

- Log distribution bar chart

A bar chart is used to display queried logs over time. You can move the cursor to a certain bar to view the number of logs hit at the time the bar represents.
- **Raw Logs**

The **Raw Logs** tab displays the results of the current query.

 - To display log data over time:
 - By default, log data in the last 15 minutes is displayed. To display data in other time, select the time range in the upper right corner.
 - To view data of all fields at a specified time, click  in front of the time in the table to expand all data. By default, data is displayed in a table.

To view data in JSON format, click the **JSON** tab. Data in JSON format is displayed on the page.
 - To display or filter some fields in the list, select the fields to be displayed in the Available Fields area on the right and click  next to the field name. The fields are displayed in the log data list on the right.
 - To adjust the field sequence: In the heading columns of the log data list on the right, select a field and then click  or  next to the field name to move the field left or right by one column with each click.
 - To cancel the display: In the table header column of the log data list on the right, select the target field, and click  next to the field name, or click  next to the field name on the left.
 - To export logs: On the **Raw Logs** tab page, click  in the upper right corner of the page. The system automatically downloads raw logs to the local PC.
- **Charts**

After a query statement is executed, you can view visualized query analysis results on the **Charts** tab.

On the **Charts** tab, SecMaster provides query and analysis results in multiple chart types, such as tables, line charts, bar charts, and pie charts. For details, see [Overview](#).
- **Alarm**

In the upper right corner of the **Analyze & Query** tab, click **Add Alarm** to add alert models. You can set alert rules for generating alerts for query and

analysis results hit the rules. For details, see [Quickly Adding a Log Alarm Model](#).

- **Quick Query**

In the upper right corner of the query analysis page, click **Save as Quick Query** to save search criteria as a quick query. For details, see [Quick Query](#).

10.5.5 Downloading Logs


SecMaster allows you to download raw logs or query and analysis logs.

Prerequisites

Data access has been completed. For details, see [Data Integration](#).

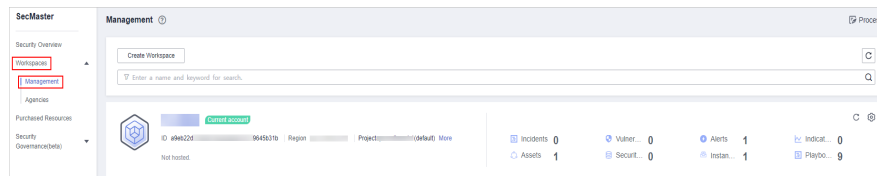
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

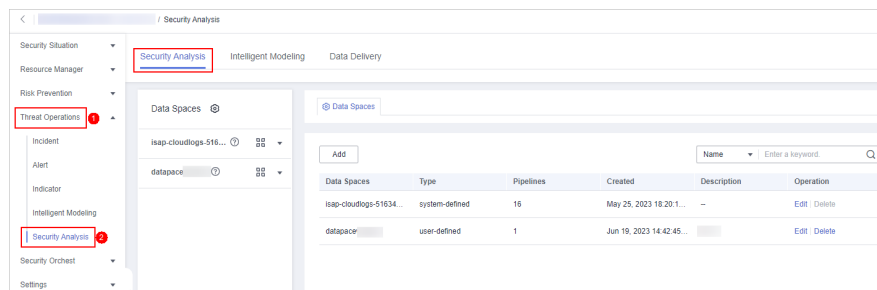
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-76 Management



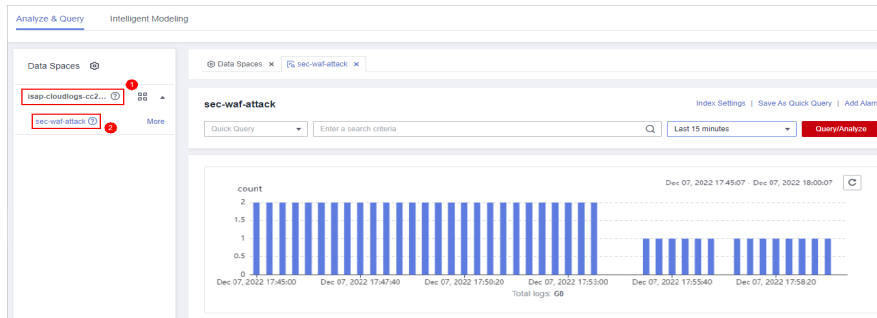
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-77 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-78 Pipeline data page



Step 6 (Optional) On the pipeline data retrieval page, enter the search criteria, select a time range, and click **Query/Analyze**.

Step 7 Download logs.

- Raw logs: On the **Raw Logs** tab page, click . The system downloads logs to the local PC.
- Chart logs: On the **Charts** tab page, click **Download**. The system downloads the logs to the local PC.

----End

10.5.6 Query and Analysis Syntax

10.5.6.1 SQL Syntax

10.5.6.1.1 Basic Syntax

An SQL statement consists of a query statement and an analysis statement, which are separated by a vertical bar (|). Query statements can be used independently, but analysis statements must be used together with query statements.

Query Statement | Analysis Statement

Table 10-25 Basic syntax

Statement Type	Description
Query Statement	A query statement is used to specify the filter criteria for log query and return the logs that meet the filter criteria. By setting filter criteria, you can quickly query required logs.
Analysis Statement	An analysis statement is used to calculate and collect statistics on query results.

10.5.6.1.2 Query Statements

A query statement is used to specify the filter criteria for log query and return the logs that meet the filter criteria. By setting filter criteria, you can quickly query required logs.

This topic describes query statements and examples.

Syntax

A query statement can be in either of the following formats:

- If the value is only *, full data is returned without filtering.
- It consists of one or more query clauses. The clauses are connected by **NOT**, **AND**, and **OR**. **()** can be used to increase the priority of the query conditions in parentheses.

The basic structure of a query clause is as follows:

Field Name Operator Field Value

Operators lists the operators that can be used.

Operators

Table 10-26 Operator descriptions

Operator	Description
=	Queries logs in which the value of a field is equal to a certain value.
<>	Queries the logs in which the value of a field is not equal to a certain value.
>	Queries logs in which the value of a field is greater than a specified value.
<	Queries logs in which the value of a field is less than a specified value.
>=	Queries logs in which the value of a field is greater than or equal to a specified value.
<=	Queries logs in which the value of a field is less than or equal to a specified value.
IN	Queries the logs whose field values are within a specified value range.
BETWEEN	Queries the logs whose field values are in the specified range.
LIKE	Searches for logs of a field value in full text.
IS NULL	Queries logs whose field value is NULL.
IS NOT NULL	Query logs whose field value is NOT NULL.

Examples

Table 10-27 Example query statements

Query Requirement	Query Statement
All logs	*
Logs about successful GET requests (status codes 200 to 299).	request_method = 'GET' AND status BETWEEN 200 AND 299
Logs of GET or POST requests	request_method = 'GET' OR request_method = 'POST'
Logs of non-GET requests	NOT request_method = 'GET'
Logs about successful GET or POST requests	(request_method = 'GET' OR request_method = 'POST') AND status BETWEEN 200 AND 299
Logs of GET or POST request failures	(request_method = 'GET' OR request_method = 'POST') NOT status BETWEEN 200 AND 299
Logs of successful GET requests (status code: 200 to 299) whose request time is greater than or equal to 60 seconds.	request_method = 'GET' AND status BETWEEN 200 AND 299 AND request_time >= 60
Logs whose request time is 60 seconds.	request_time = 60

10.5.6.1.3 Analysis Statements

Syntax of Analysis Statements

The syntax of a complete analysis statement is as follows:

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

SELECT

Specifies the field to be queried.

Using * to query all fields.

```
SELECT *
```

Table 10-28 Using * to query all fields

account_number	firstname	gender	city	balance	employer	state	lastname	age
1	Amber	M	Brogan	39225	Pyrami	IL	Duke	32
16	Hattie	M	Dante	5686	Netagy	TN	Bond	36
13	Nanette	F	Nogal	32838	Quility	VA	Bates	28
18	Dale	M	Orick	4180	null	MD	Adams	32

Querying a Specified Field

```
SELECT firstname, lastname
```

Table 10-29 Querying a Specified Field

firstname	lastname
Amber	Duke
Hattie	Bond
Nanette	Bates
Dale	Adams

Using AS to Define Field Aliases

```
SELECT account_number AS num
```

Table 10-30 Using AS to define field aliases

num
1
16
13
18

Using the DISTINCT Statement

```
SELECT DISTINCT age
```

Table 10-31 Using the DISTINCT statement

age
32
36
28

Using SQL Functions

For details about functions, see [Functions](#).

```
SELECT LENGTH(firstname) as len, firstname
```

Table 10-32 Using SQL functions

len	firstname
4	Amber
6	Hattie
7	Nanette
4	Dale

GROUP BY

Groups data by field value.

Grouping by Field Value

```
SELECT age GROUP BY age
```

Table 10-33 Grouping by field value

age
28
32
36

Grouping by Field Alias

```
SELECT account_number AS num GROUP BY num
```

Table 10-34 Grouping by field alias

num
1
16
13
18

Grouping by Multiple Fields

```
SELECT account_number AS num, age GROUP BY num, age
```

Table 10-35 Grouping by multiple fields

num	age
1	32
16	36
13	28
18	32

Using SQL Functions

For details about functions, see [Function](#).

```
SELECT LENGTH(lastname) AS len, COUNT(*) AS count GROUP BY LENGTH(lastname)
```

Table 10-36 Using SQL functions

len	count
4	2
5	2

HAVING

Filters data based on grouping and [Aggregate Functions](#).

```
SELECT age, MAX(balance) GROUP BY age HAVING MIN(balance) > 10000
```

Table 10-37 The HAVING function

age	MAX(balance)
28	32838
32	39225

ORDER BY

Sorts data by field value.

Sorting Data by Field Value

```
SELECT age ORDER BY age DESC
```

Table 10-38 Sorting by field value

age
28
32
32
36

LIMIT

Specifies the number of returned data records.

Specifying the Number of Returned Records

```
SELECT * LIMIT 1
```

Table 10-39 Specifying the number of returned records

account_number	first name	gender	city	balance	employer	state	last name	age
1	Amber	M	Brogan	39225	Pyrami	IL	Duke	32

Specifying the Number of Returned Records and Offsets

```
SELECT * LIMIT 1 OFFSET 1
```

Table 10-40 Specifying the number of returned records and offsets

account_number	first_name	gender	city	balance	employer	state	last_name	age
16	Hattie	M	Dante	5686	Netag y	TN	Bond	36

Functions

Mathematics Functions

Table 10-41 Mathematics Functions

Function	Purpose	Description	Example Value
abs	Absolute value	abs(number T) -> T	SELECT abs(0.5) LIMIT 1
add	Addition	add(number T, number) -> T	SELECT add(1, 5) LIMIT 1
cbrt	Cubic root	cbrt(number T) -> T	SELECT cbrt(0.5) LIMIT 1
ceil	Rounded up	ceil(number T) -> T	SELECT ceil(0.5) LIMIT 1
divide	Division	divide(number T, number) -> T	SELECT divide(1, 0.5) LIMIT 1
e	Natural base number e	e() -> double	SELECT e() LIMIT 1
exp	Power of the natural base number e	exp(number T) -> T	SELECT exp(0.5) LIMIT 1
expm1	Subtract one from the power of the natural base number e.	expm1(number T) -> T	SELECT expm1(0.5) LIMIT 1
floor	Rounded down	floor(number T) -> T	SELECT floor(0.5) AS Rounded_Down LIMIT 1
ln	Returns the natural logarithm.	ln(number T) -> double	SELECT ln(10) LIMIT 1
log	Logarithm with T as the base	log(number T, number) -> double	SELECT log(10) LIMIT 1

Function	Purpose	Description	Example Value
log2	Logarithm with 2 as the base	log2(number T) -> double	SELECT log2(10) LIMIT 1
log10	Logarithm to base 10	log10(number T) -> double	SELECT log10(10) LIMIT 1
mod	Remainder	mod(number T, number) -> T	SELECT modulus(2, 3) LIMIT 1
multiply	Multiplication	multiply(number T, number) -> number	SELECT multiply(2, 3) LIMIT 1
pi	π	pi() -> double	SELECT pi() LIMIT 1
pow	T power of	pow(number T, number) -> T	SELECT pow(2, 3) LIMIT 1
power	T power of	power(number T) -> T, power(number T, number) -> T	SELECT power(2, 3) LIMIT 1
rand	Random number.	rand() -> number, rand(number T) -> T	SELECT rand(5) LIMIT 1
rint	Discard decimals.	rint(number T) -> T	SELECT rint(1.5) LIMIT 1
round	Round off	round(number T) -> T	SELECT round(1.5) LIMIT 1
sign	Symbol	sign(number T) -> T	SELECT sign(1.5) LIMIT 1
signum	Symbol	signum(number T) -> T	SELECT signum(0.5) LIMIT 1
sqrt	Square root	sqrt(number T) -> T	SELECT sqrt(0.5) LIMIT 1
subtract	Subtraction	subtract(number T, number) -> T	SELECT subtract(3, 2) LIMIT 1
/	Division	number / number -> number	SELECT 1 / 100 LIMIT 1
%	Remainder	number % number -> number	SELECT 1 % 100 LIMIT 1

Trigonometric Functions

Table 10-42 Trigonometric functions

Function s	Purpose	Description	Example Value
acos	Arc cosine	acos(number T) -> double	SELECT acos(0.5) LIMIT 1
asin	Arc sine	asin(number T) -> double	SELECT asin(0.5) LIMIT 1
atan	Inverse tangent	atan(number T) -> double	SELECT atan(0.5) LIMIT 1
atan2	T Arc tangent of the result of dividing U	atan2(number T, number U) -> double	SELECT atan2(1, 0.5) LIMIT 1
cos	Cosine	cos(number T) -> double	SELECT cos(0.5) LIMIT 1
cosh	hyperbolic cosine	cosh(number T) -> double	SELECT cosh(0.5) LIMIT 1
cot	Cotangent	cot(number T) -> double	SELECT cot(0.5) LIMIT 1
degrees	Converting radians to degrees	degrees(number T) -> double	SELECT degrees(0.5) LIMIT 1
radians	Converting degrees to radians	radians(number T) -> double	SELECT radians(0.5) LIMIT 1
sin	Sine	sin(number T) -> double	SELECT sin(0.5) LIMIT 1
sinh	hyperbolic sine	sinh(number T) -> double	SELECT sinh(0.5) LIMIT 1
tan	Tangent	tan(number T) -> double	SELECT tan(0.5) LIMIT 1

Temporal Functions

Table 10-43 Temporal functions

Function	Purpose	Description	Example Value
curdate	Specifies the current date.	curdate() -> date	SELECT curdate() LIMIT 1
date	Date	date(date) -> date	SELECT date() LIMIT 1
date_format	Obtains the date value based on the format.	date_format(date, string) -> string	SELECT date_format(date, 'Y') LIMIT 1
day_of_month	Month	day_of_month(date) -> integer	SELECT day_of_month(date) LIMIT 1
day_of_week	Day of a week	day_of_week(date) -> integer	SELECT day_of_week(date) LIMIT 1
day_of_year	Number of days in the current year	day_of_year(date) -> integer	SELECT day_of_year(date) LIMIT 1
hour_of_day	Number of hours on the current day	hour_of_day(date) -> integer	SELECT hour_of_day(date) LIMIT 1
maketime	Date of Generation	maketime(integer, integer, integer) -> time	SELECT maketime(11, 30, 00) LIMIT 1
minute_of_hour	Number of minutes in the current hour	minute_of_hour(date) -> integer	SELECT minute_of_hour(date) LIMIT 1
minute_of_day	Number of minutes on the current day	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
monthname	Month Name	monthname(date) -> string	SELECT monthname(date) LIMIT 1
now	Current time.	now() -> time	SELECT now() LIMIT 1
second_of_minute	Number of seconds	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
timestamp	Date	timestamp(date) -> date	SELECT timestamp(date) LIMIT 1

Function	Purpose	Description	Example Value
year	Year	year(date) -> integer	SELECT year(date) LIMIT 1

Text Functions

Table 10-44 Text functions

Function	Purpose	Description	Example Value
ascii	ASCII value of the first character	ascii(string T) -> integer	SELECT ascii('t') LIMIT 1
concat_ws	Connection String	concat_ws(separator, string, string) -> string	SELECT concat_ws('-', 'Tutorial', 'is', 'fun!') LIMIT 1
left	Obtain a character string from left to right.	left(string T, integer) -> T	SELECT left('hello', 2) LIMIT 1
length	length	length(string) -> integer	SELECT length('hello') LIMIT 1
locate	Search for a string	locate(string, string) -> integer	SELECT locate('o', 'hello') LIMIT 1
replace	Replace strings	replace(string T, string, string) -> T	SELECT replace('hello', 'l', 'x') LIMIT 1
right	Obtain a character string from right to left.	right(string T, integer) -> T	SELECT right('hello', 1) LIMIT 1
rtrim	Remove the empty character string on the right.	rtrim(string T) -> T	SELECT rtrim('hello ') LIMIT 1
substring	Obtaining a Substring	substring(string T, integer, integer) -> T	SELECT substring('hello', 2,5) LIMIT 1
trim	Remove empty character strings on both sides.	trim(string T) -> T	SELECT trim(' hello ') LIMIT 1

Function	Purpose	Description	Example Value
upper	Convert all letters to uppercase letters.	upper(string T) -> T	SELECT upper('helloworld') LIMIT 1

Other

Table 10-45 Other

Function	Purpose	Description	Example Value
if	if condition	if(boolean, object, object) -> object	SELECT if(false, 0, 1) LIMIT 1 , SELECT if(true, 0, 1) LIMIT 1
ifnull	If the field is null, the default value is used.	ifnull(object, object) -> object	SELECT ifnull('hello', 1) LIMIT 1 , SELECT ifnull(null, 1) LIMIT 1
isnull	Indicates whether a field is null. If yes, 1 is returned. If no, 0 is returned.	isnull(object) -> integer	SELECT isnull(null) LIMIT 1 , SELECT isnull(1) LIMIT 1

Aggregate Functions

Table 10-46 Aggregate functions

Function	Purpose	Description	Example Value
avg	Average value	avg(number T) -> T	SELECT avg(age) LIMIT 1
sum	Sum	sum(number T) -> T	SELECT sum(age) LIMIT 1
min	Specifies the minimum value.	min(number T) -> T	SELECT min(age) LIMIT 1
max	Maximum value	max(number T) -> T	SELECT max(age) LIMIT 1

Function	Purpose	Description	Example Value
count	Occurrences	count(field) -> integer , count(*) -> integer , count(1) -> integer	SELECT count(age) LIMIT 1 , SELECT count(*) LIMIT 1 , SELECT count(1) LIMIT 1

10.5.6.1.4 Limitations and Constraints

- Query statements do not support mathematical operations, such as $(age + 100) \leq 1000$.
- Aggregate functions support only fields and do not support expressions, for example, $avg(\log(age))$.
- Multi-table association is not supported.
- Subqueries are not supported.
- A maximum of 500 records can be returned on the page.
- A maximum of 10,000 groups can be returned by GROUP BY.

10.5.6.2 Quick Query

Quick Query is a function of SecMaster that provides saved query and analysis operations. You can save a common query and analysis statement as a quick query statement for future use.

This topic describes how to create a quick query.

Prerequisites

Indexes have been configured. For details, see [Configuring Indexes](#).

Creating a Quick Query


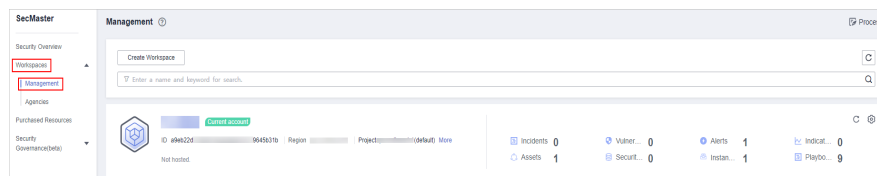
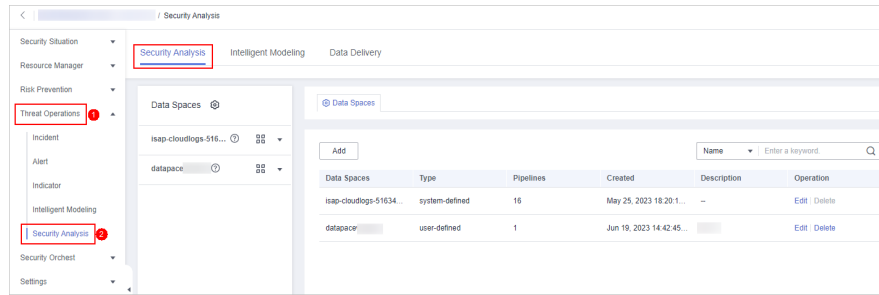
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-79 Management



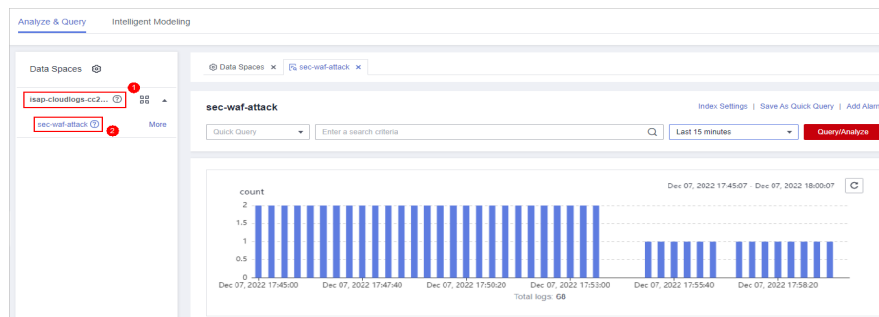
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-80 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-81 Pipeline data page



Step 6 Enter the query and analysis statement, set the time range, and click **Query/Analyze**.

For details, see [Querying and Analyzing Data](#).

Step 7 Click **Save as Quick Query** in the upper right corner of the area, configure query parameters on the right, and click **OK**.

Figure 10-82 Save As Quick Query




Table 10-47 Parameters for a quick query

Parameter	Description
Query Name	Set the name of the quick query.

Parameter	Description
Query statement	The system automatically generates the query statement entered in Step 6 .

Step 8 Click **OK**.

After creating a quick query, you can click  in the quick query search box on the pipeline data query and analysis page and select the target quick query name to use the quick query.

----End

10.5.7 Quickly Adding a Log Alarm Model

SecMaster allows you to set alarm models for query and analysis results and trigger alarms when conditions are met.


This topic describes how to quickly configure alarm models for logs.

Prerequisites

Data access has been completed. For details, see [Data Integration](#).

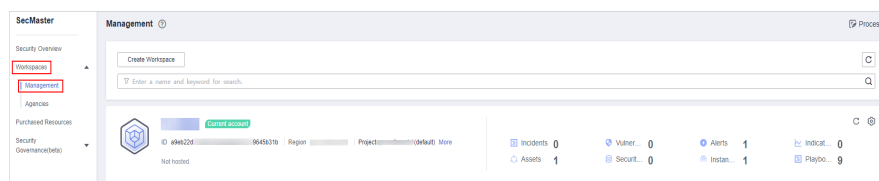
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

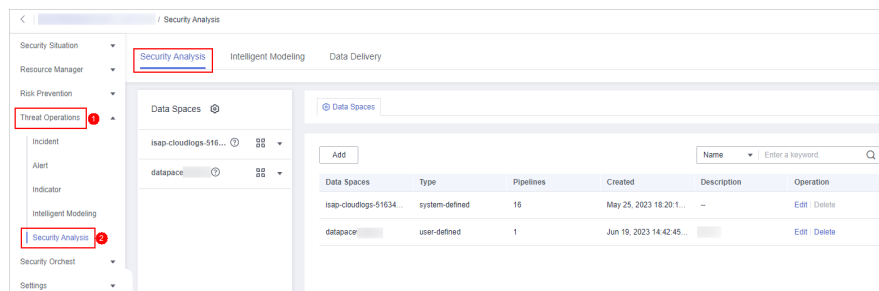
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-83 Management



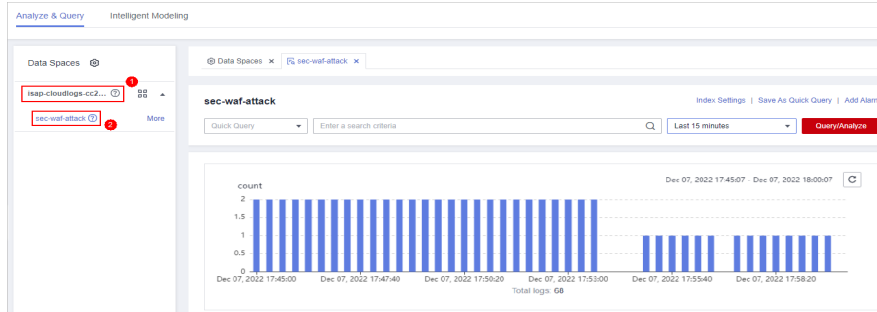
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-84 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-85 Pipeline data page

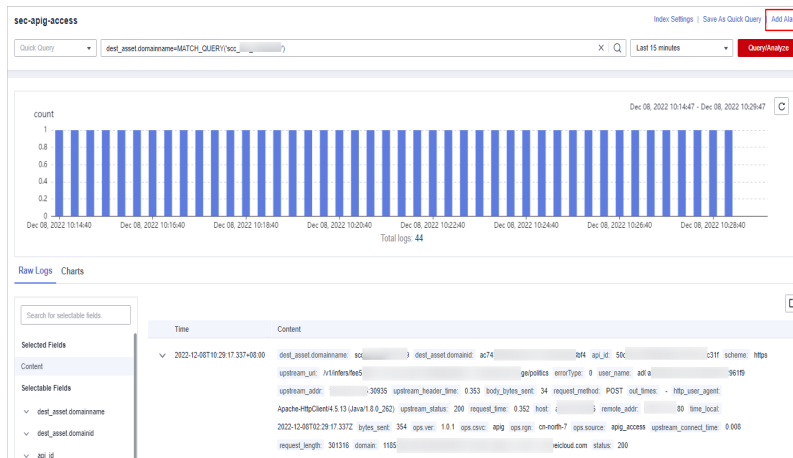


Step 6 Enter the query analysis statement, set the time range, and click **Query/Analyze**. The query analysis result is displayed.

For details, see [Querying and Analyzing Data](#).

Step 7 Click **Add Alarm** in the upper right corner of the page. The **Create Alarm Model** page is displayed.



Figure 10-86 Add Alarm



Step 8 Configure basic alarm information by referring to [Table 10-48](#).

Figure 10-87 Basic configuration



Table 10-48 Basic parameters of an alarm model

Parameter	Description
Pipeline Name	The pipeline where the alert model is executed, which is generated by the system by default.
Model Name	Name of the alarm model.
Severity	Severity of alarms reported by the alarm model. You can set the severity to Critical , High , Medium , Low , or Informative .
Alarm Type	Alarm type displayed after the alarm model is triggered.
Model Type	The default value is Rule model .
Description	Enter the description of the alarm model.
Status	<p>The alarm model status.</p> <ul style="list-style-type: none">  : indicates that the model is enabled. This is the default status.  : indicates that the model is disabled. You can change the alarm model status after the model is configured.

Step 9 After the setting is complete, click **Next** in the lower right corner of the page. The page for setting the model logic is displayed.

Step 10 Set the model logic. For details about the parameters, see [Table 10-49](#).

Table 10-49 Configure Model Logic

Parameter	Description
Query Rule	Set alert query rules. After the setting is complete, click Run and view the running result.
Query Plan	<p>Set an alert query plan.</p> <ul style="list-style-type: none"> Running query interval: xx minutes/hour/day. If the running query interval is minute, set this parameter to a value ranging from 5 to 59 minutes. If the running query interval is hour, set this parameter to a value ranging from 1 to 23 hours. If the running query interval is day, set this parameter to a value ranging from 1 to 14 days. Time window: xx minutes/hour/day. If the time window is minute, the value ranges from 5 minutes to 59 minutes. If the time window is hour, the value ranges from 1 hour to 23 hours. If the time window is day, the value ranges from 1 day to 14 days. Execution Delay: xx minutes. The value ranges from 0 to 5 minutes.
Advanced Alarm Settings	<ul style="list-style-type: none"> Custom Information: Customize extended alert information. Click Add, and set the key and value information. Alarm Details: Enter the alarm name, description, and handling suggestions.
Trigger Condition	<p>Sets alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx.</p> <p>If there are multiple triggers, click Add.</p>
Alarm Trigger	<p>The way to trigger alerts for queried results. The options are as follows:</p> <ul style="list-style-type: none"> One alert for all query results One alert for each query result
Debugging	Sets whether to generate debugging alarms.
Suppression	<p>Specifies whether to stop the query after an alert is generated.</p> <ul style="list-style-type: none">  : indicates that the query stops after an alert is generated.  : indicates that the query is not stopped after an alert is generated.

Step 11 After the setting is complete, click **Next** in the lower right corner of the page. The model details preview page is displayed.

Step 12 After confirming that the preview is correct, click **OK** in the lower right corner of the page to confirm the configuration.

----End

10.5.8 Charts

10.5.8.1 Overview

After you run query and analysis statements, SecMaster can display the query and analysis results in charts and tables. You can save indicators as cards for future use in the layout.

Currently, the following chart types are supported:

- **Chart**
- **Line Chart**
- **Bar Chart**
- **Pie Chart**


10.5.8.2 Tables

The query and analysis results can be displayed in a table.

Table is the most commonly used method to display and analyze data. In SecMaster, the data results obtained by querying and analyzing statements are displayed in tables by default.

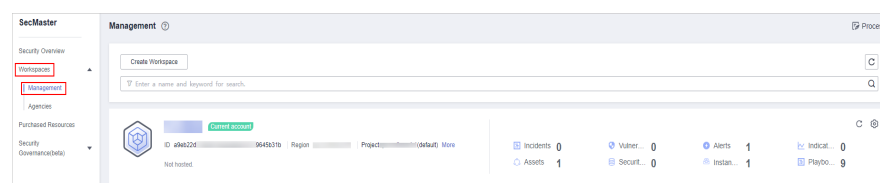
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

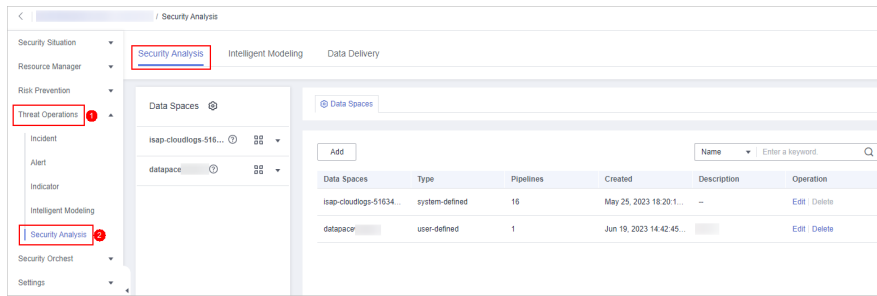
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-88 Management



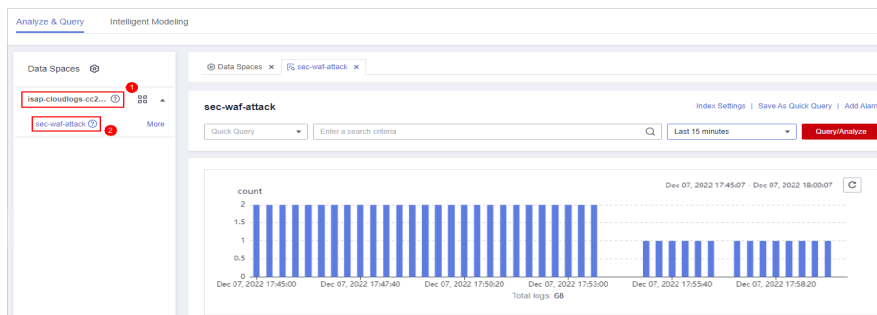
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-89 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

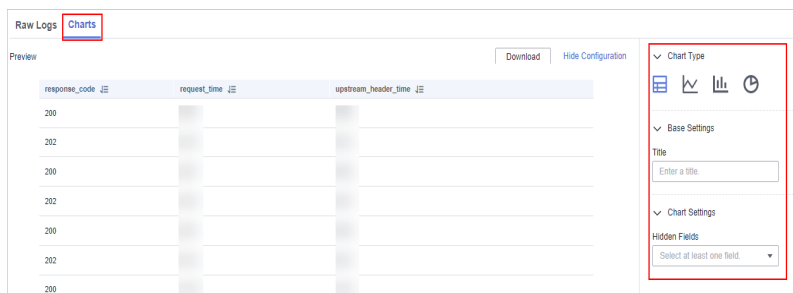
Figure 10-90 Pipeline data page



Step 6 Enter the query and analysis statement, set the time range, and click **Query/Analyze**.

Step 7 Click the **Charts** tab. In the **Chart Type** area on the right of the page, click .

Figure 10-91 Charts



Step 8 Set parameters in the table.

Table 10-50 Table parameters

Category	Parameter	Description
Base Settings	Title	Customize the table title.
Chart Settings	Hidden Fields	Select a target field to hide it in the table.

After the chart is configured, you can preview the configured data analysis on the left.

----End

Related Operations

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click **Add as Indicator Card** in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click **Save**.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.
- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.


10.5.8.3 Line Charts

The query and analysis results can be displayed in a line chart.

A line chart is used to display the change of a group of data in a period and show the data change trend.

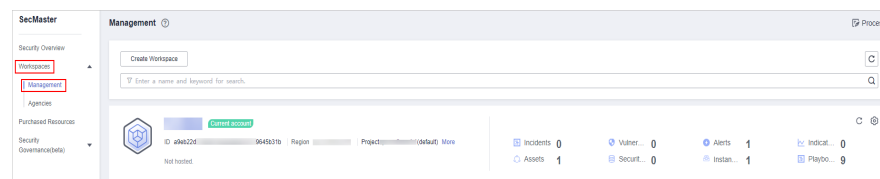
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

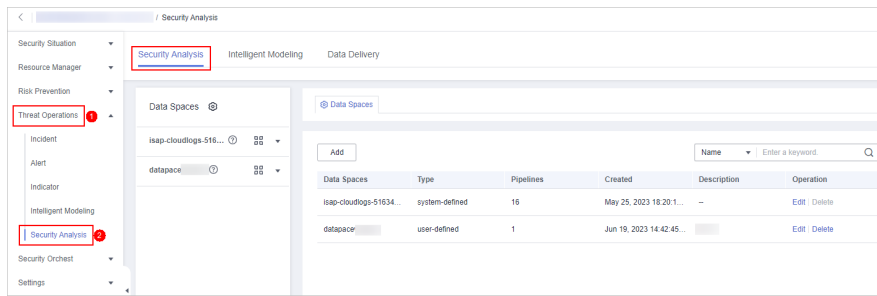
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-92 Management



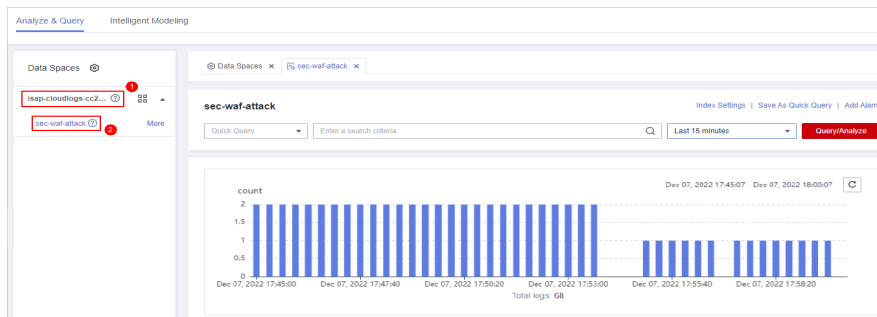
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-93 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

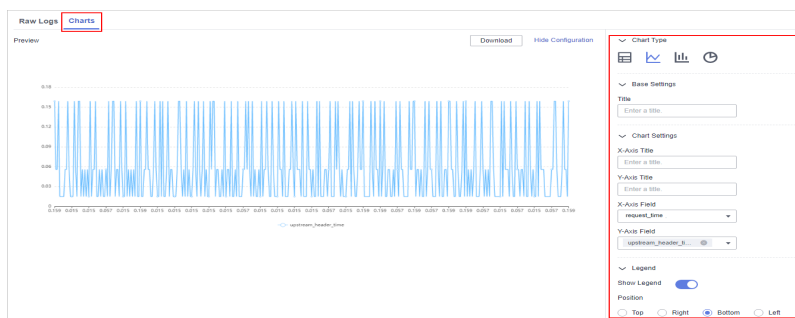
Figure 10-94 Pipeline data page



Step 6 Enter the query and analysis statement, set the time range, and click **Query/Analyze**.

Step 7 Click the **Charts** tab. In the **Chart Type** area on the right of the page, click .

Figure 10-95 Line chart statistics



Step 8 Set line chart parameters.

Table 10-51 Line chart parameters

Category	Parameter	Description
Base Settings	Title	Customized line chart title
Chart Settings	X-Axis Title	Customized title of the X axis

Category	Parameter	Description
	Y-Axis Title	Customized title of the Y axis
	X-Axis Field	Field to be displayed on the X axis
	Y-Axis Field	Field to be displayed on the Y axis
Legend	Show Legend	Determine whether to display the legend.
	Position	This parameter is mandatory when the legend display function is enabled. Position of the legend in the chart. The options are Top , Bottom , Left , and Right .

After the chart is configured, you can preview the configured data analysis result on the left.

----End

Related Operations

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click **Add as Indicator Card** in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click **Save**.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.
- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.


10.5.8.4 Bar Charts

The query and analysis results can be displayed in a bar chart.

A bar chart presents categorical data with rectangular bars with heights or lengths. It can be used to compare data and trends. In SecMaster, the bar chart uses vertical bars (the width is fixed and the height indicates the value) to display data by default.

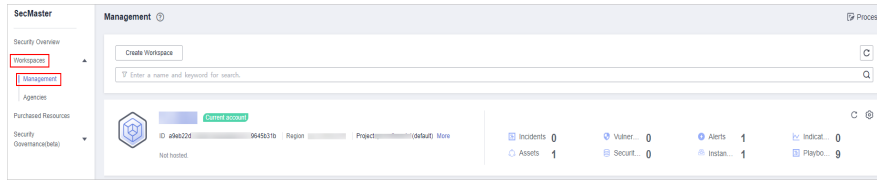
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

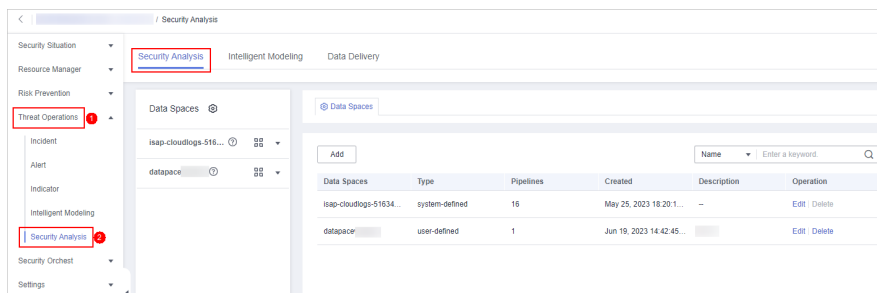
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-96 Management



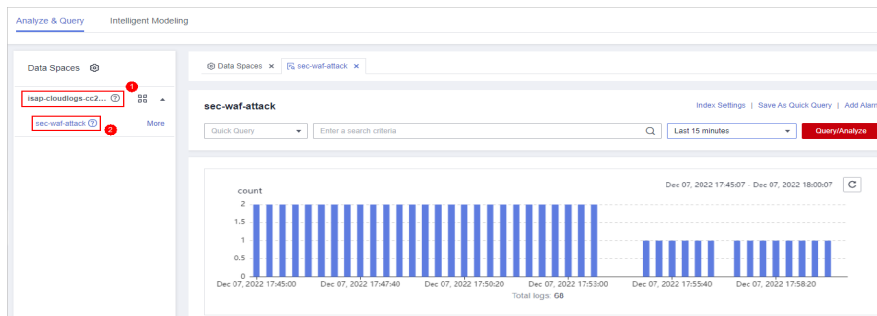
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-97 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-98 Pipeline data page



Step 6 Enter the query and analysis statement, set the time range, and click **Query/Analyze**.

Step 7 Click the **Charts** tab. In the **Chart Type** area on the right of the page, click .

Figure 10-99 Bar chart statistics



Step 8 Set bar chart parameters.

Table 10-52 Bar chart parameters

Category	Parameter	Description
Base Settings	Title	Customized line chart title
Chart Settings	X-Axis Title	Customized title of the X axis
	Y-Axis Title	Customized title of the Y axis
	X-Axis Field	Field to be displayed on the X axis
	Y-Axis Field	Field to be displayed on the Y axis
Legend	Show Legend	Determine whether to display the legend.
	Position	This parameter is mandatory when the legend display function is enabled. Position of the legend in the chart. The options are Top , Bottom , Left , and Right .

After the chart is configured, you can preview the configured data analysis result on the left.

----End

Related Operations

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click **Add as Indicator Card** in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click **Save**.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.

- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.

10.5.8.5 Pie Charts

The query and analysis results can be displayed in a pie chart.

The pie chart is used to show the proportion of different categories. Different categories are compared by radian.

Procedure


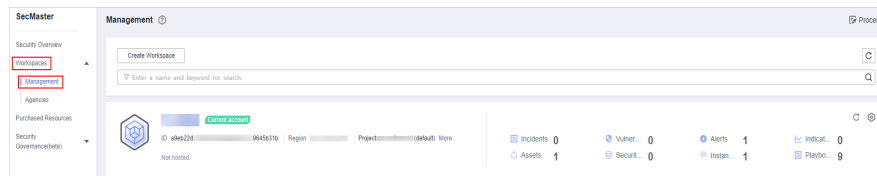
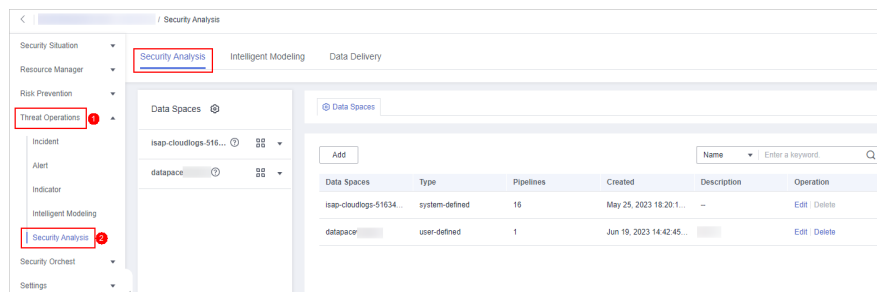
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-100 Management



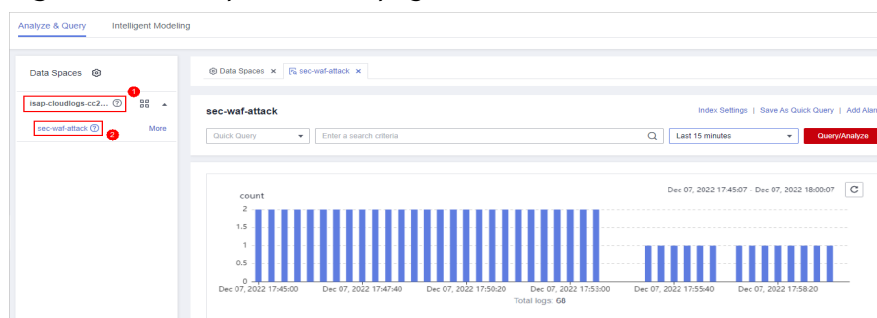
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-101 Accessing the Security Analysis tab page



- Step 5** In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

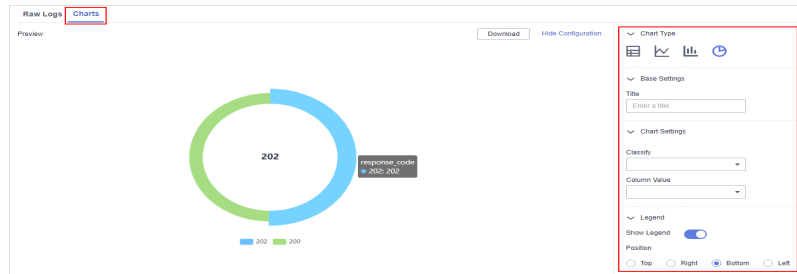
Figure 10-102 Pipeline data page



Step 6 Enter the query and analysis statement, set the time range, and click **Query/Analyze**.

Step 7 Click the **Charts** tab. In the **Chart Type** area on the right of the page, click .

Figure 10-103 Pie chart statistics



Step 8 Set pie chart parameters.

Table 10-53 Pie chart parameters

Category	Parameter	Description
Base Settings	Title	Customized line chart title
Chart Settings	Classify	Data classification
	Column Value	Value of the data type
Legend	Show Legend	Determine whether to display the legend.
	Position	This parameter is mandatory when the legend display function is enabled. Position of the legend in the chart. The options are Top , Bottom , Left , and Right .

After the chart is configured, you can preview the configured data analysis result on the left.

----End

Related Operations

- Adding an indicator card: After the configuration, if you want to save the indicator information as a card, click **Add as Indicator Card** in the upper right corner of the table to add an indicator card. In the dialog box that is displayed, set the indicator card name and click **Save**.
- Download logs: After the chart configuration, you can click **Download** in the upper right corner of the table to download the current query analysis data to the local PC.
- Hide configuration: After the chart configuration, you can click **Hide Configuration** on the right of the **Preview** to hide the parameters.

- Show configuration: After the chart configuration is hidden, you can click **Show Configuration** on the right of **Preview** to expand and set parameters.

10.5.9 Managing Data Spaces

10.5.9.1 Creating a Data Space

A data space is a unit for data grouping, load balancing, and flow control. Data in the same data space shares the same load balancing policy.

When you need to use the security analysis, data analysis, and intelligent modeling features provided by SecMaster, you need to create a data space.

This section describes how to create a data space.

Prerequisites

A workspace has been created. For details, see [Creating a Workspace](#).

Limitations and Constraints

A maximum of five data spaces can be created in a workspace.

Procedure


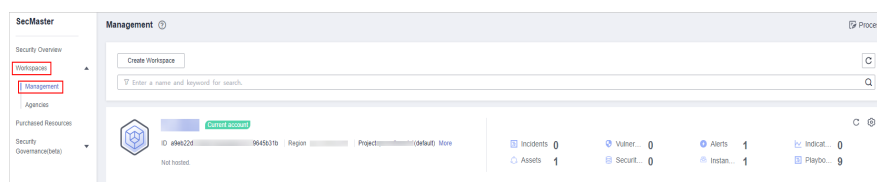
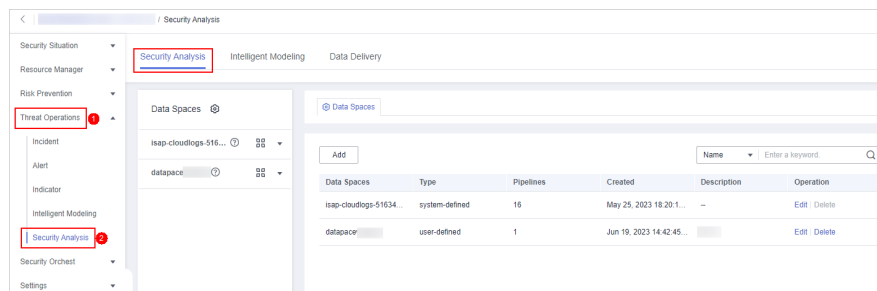
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-104 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-105 Accessing the Security Analysis tab page



Step 5 In the upper left corner of the data space list, click **Add**. The **Adding Data Spaces** page is displayed on the right.

Figure 10-106 Adding a data space



Step 6 On the **Adding Data Spaces** page, set the parameters for the new data space. For details about the parameters, see [Table 10-54](#).

Table 10-54 Adding a data space

Parameter	Description
Data Space	Data space name. It must meet the following requirements: <ul style="list-style-type: none"> The name contains 5 to 63 characters. The value can contain letters, numbers, and hyphens (-). The hyphen (-) cannot be used at the beginning or end, or used consecutively. The name must be unique and cannot be the same as any other data space name.
Description	You can make remarks on the data space. This parameter is optional.

Step 7 Click **OK**. The data space is added.

After the data space is added, you can view the new data space in the data space list.


----End

10.5.9.2 Viewing Data Space Details

This topic describes how to view the information about a data space, including the name, type, and creation time.

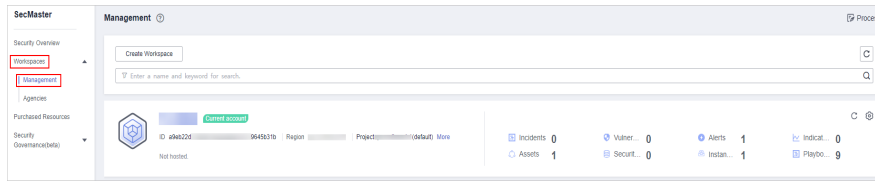
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

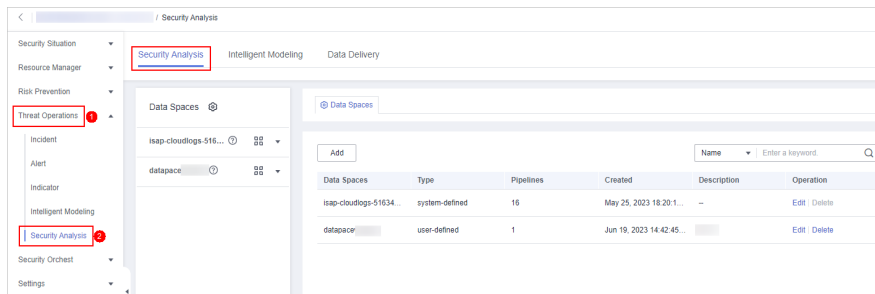
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-107 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-108 Accessing the Security Analysis tab page



Step 5 On the **Data Spaces** page, view all data space information. **Table 10-55** describes related parameters.

Table 10-55 Data space parameters

Parameter	Description
Data Spaces	Data space name
Type	Type of data in the data space. It may be: <ul style="list-style-type: none"> System-defined: data space created by the system by default during data access. User-defined: data space created by users.
Pipelines	Number of pipelines in the data space.
Created	Time when the data space is created.
Description	Description of the data space
Operation	You can perform operations such as editing and deleting in the Operation column.


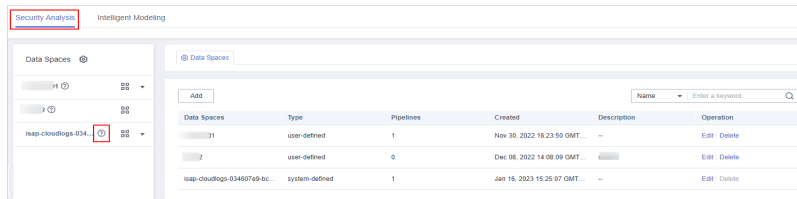
Step 6 In the data space column on the left, click  next to a data space name to view the details about the data space.

Figure 10-109 Data space details



Step 7 In the **Data Space Details** area, you can view details about a data space. For details about the parameters, see [Table 10-56](#).

Table 10-56 Data space details

Parameter	Description
Data Spaces	Data space name
Pipelines	Number of pipelines in the data space.
Created	Time when the data space is created.
Description	Description of the data space

----End

10.5.9.3 Editing a Data Space

This topic describes how to modify the information of a data space after the data space is created.

Procedure


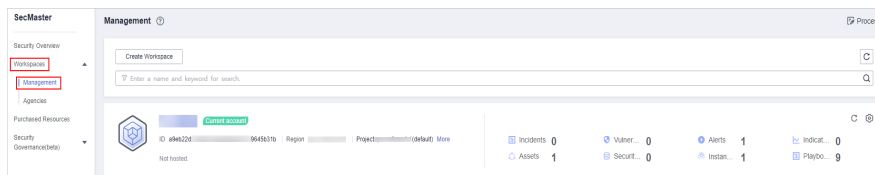
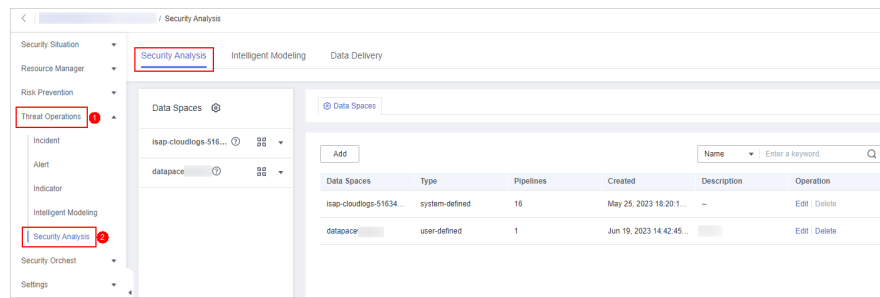
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-110 Management



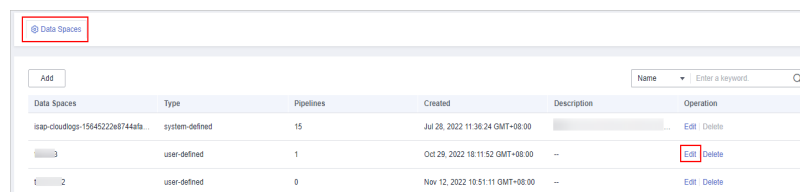
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-111 Accessing the Security Analysis tab page



Step 5 Locate the row that contains the data space to be edited, and click **Edit** in the **Operation** column.

Figure 10-112 Editing a data space



Step 6 In the displayed **Edit Data Space** dialog box, modify the data space information.

Step 7 Click **OK**.

----End

10.5.9.4 Deleting a Data Space


This topic describes how to delete a data space that is no longer needed.

Limitations and Constraints

- The default data space created by the system cannot be deleted.
- If a pipeline exists in the data space to be deleted, the data space cannot be deleted directly. You need to delete the pipeline before deleting the data space.

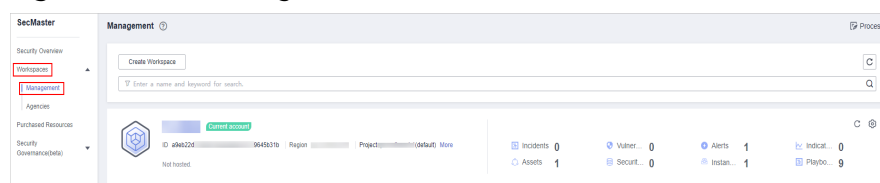
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

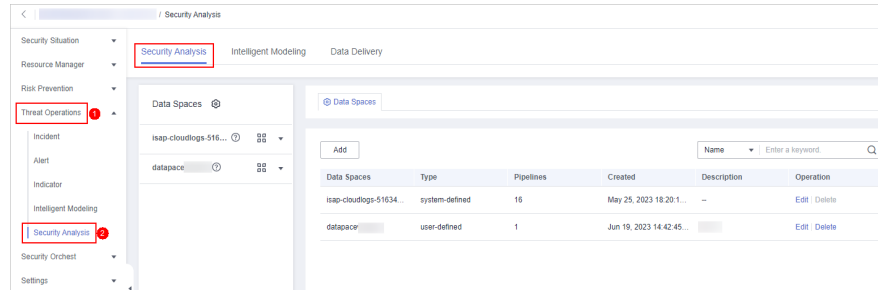
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-113 Management



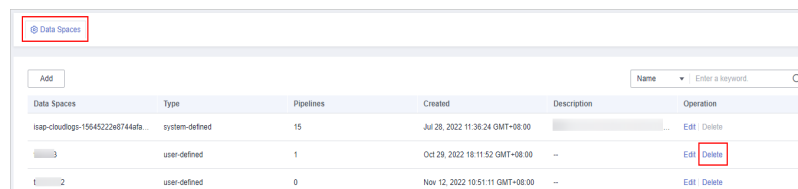
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-114 Accessing the Security Analysis tab page



Step 5 In the row containing the desired database, click **Delete** in the **Operation** column.

Figure 10-115 Deleting a data space



Step 6 In the dialog box that is displayed, click **OK**. The data space is deleted.

CAUTION

If a pipeline exists in the data space to be deleted, the data space cannot be deleted directly. You need to delete the pipeline before deleting the data space.

----End

10.5.10 Managing Pipelines

10.5.10.1 Creating a Pipeline

A data transfer message topic and a storage index form a pipeline.

To use the security analysis, data analysis, and intelligent modeling functions provided by SecMaster, you need to create pipelines.

This section describes how to create a pipeline.

Prerequisites

- A workspace has been created. For details, see [Creating a Workspace](#).
- A data space has been added. For details, see [Creating a Data Space](#).

Limitations and Constraints

A maximum of 20 pipelines can be created in a data space.

Procedure


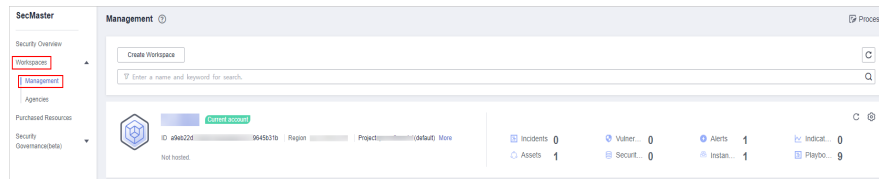
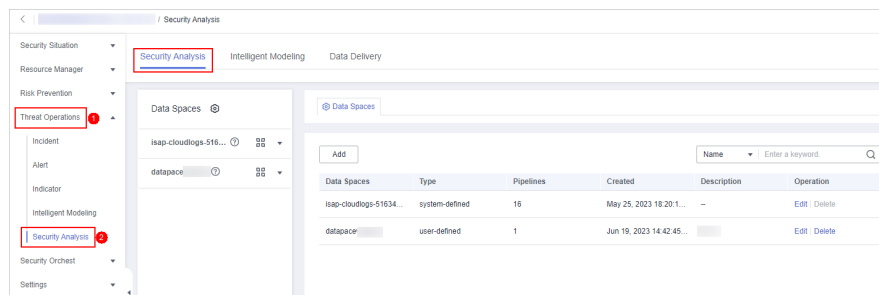
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-116 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-117 Accessing the Security Analysis tab page




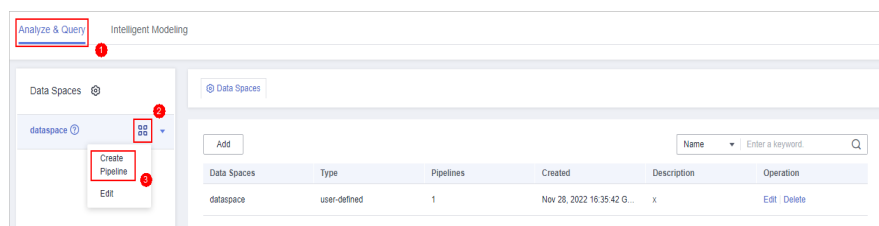
- Step 5** In the data space navigation pane on the left, click  on the right of the data space name and select **Create Pipeline** from the drop-down list box. The **Create Pipeline** page is displayed on the right.

Figure 10-118 Creating a pipeline



- Step 6** On the **Create Pipeline** page, configure pipeline parameters. For details about the parameters, see [Table 10-57](#).

Table 10-57 Creating a pipeline

Parameter	Description
Data Spaces	Data space to which the pipeline belongs.

Parameter	Description
Pipeline Name	Name of the pipeline. It must meet the following requirements: <ul style="list-style-type: none"> The name contains 5 to 63 characters. The value can contain letters, numbers, and hyphens (-). The hyphen (-) cannot be used at the beginning or end, or used consecutively. The name must be unique in the data space.
Shards	The number of shards of the pipeline. The value range is 1 to 64.
Lifecycle	Life cycle of data in the pipeline. Value range: 7-180
Description	Remarks on the pipeline. This parameter is optional.

Step 7 Click **OK**.

After the pipeline is created, you can click the data space name or ▼ next to the data space to view the created pipeline.


----End

10.5.10.2 Viewing Pipeline Details

This topic describes how to view the pipeline details, including the pipeline name, data space, and creation time.

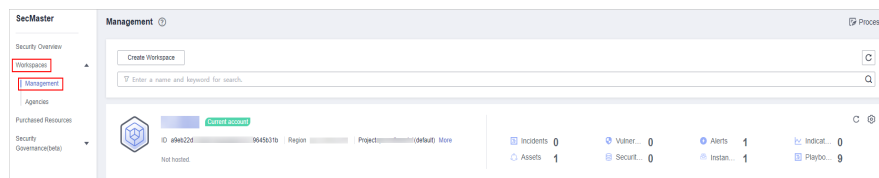
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

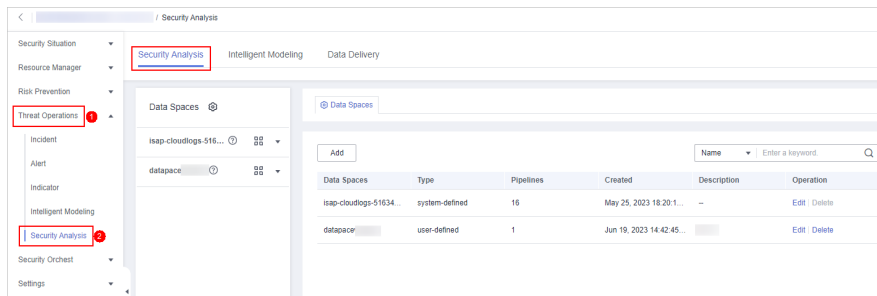
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-119 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-120 Accessing the Security Analysis tab page




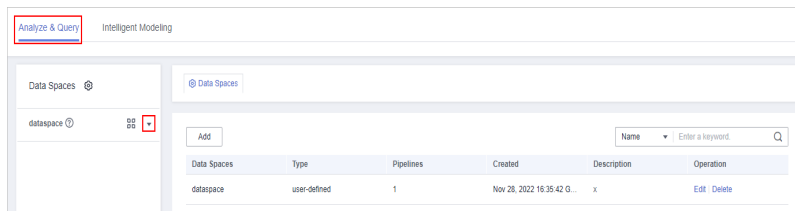
Step 5 In the data space navigation tree on the left, click the data space name or  to view the created pipeline.

Figure 10-121 Viewing pipeline details




Step 6 Click  next to a pipeline name you want to view. The pipe details are displayed in the right pane.

Table 10-58 Pipeline parameters

Parameter	Description
Workspace Name	Name of the workspace to which the current pipe belongs.
Workspace ID	ID of the workspace to which the current pipe belongs.
Data Space Name	Name of the data space to which the current pipeline belongs.
Data Space ID	ID of the data space to which the current pipeline belongs.
Pipeline Name	Name of the current pipeline.
Pipeline ID	ID of the current pipeline.
Shards	Number of shards of the pipeline.
Lifecycle	Retention period of data in the pipeline.
Created	Time when a pipe is created
Description	Description of the pipeline

----End

10.5.10.3 Editing a Pipeline

After a pipeline is created, you can modify the pipeline information, such as number of shards, description, and lifecycle.

Limitations and Constraints

Pipelines created by the system cannot be edited.

Procedure


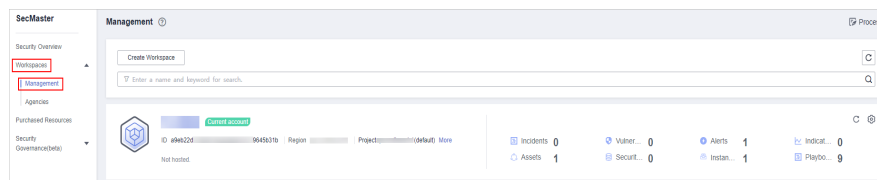
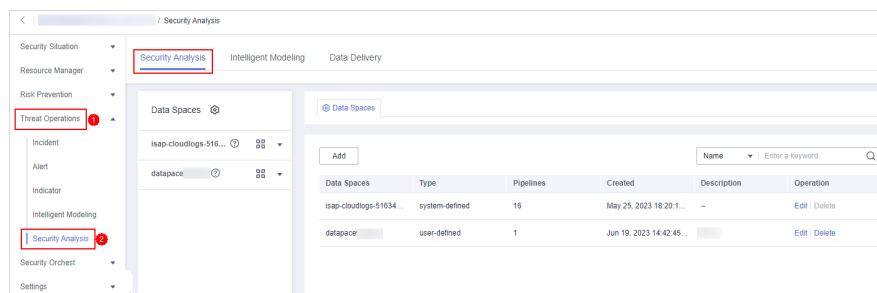
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-122 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-123 Accessing the Security Analysis tab page




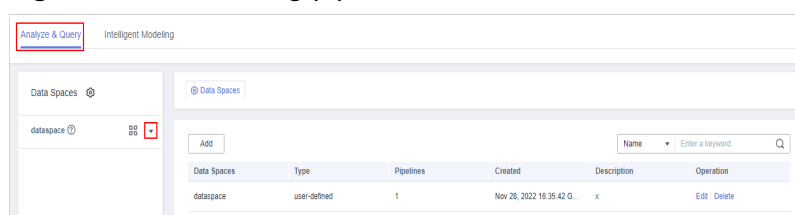
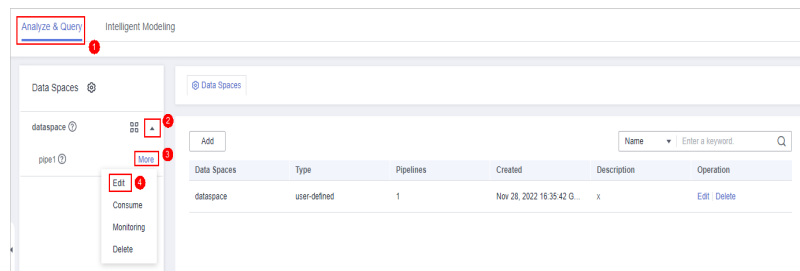
- Step 5** In the data space navigation tree on the left, click the data space name or  to view the created pipeline.

Figure 10-124 Viewing pipeline details



- Step 6** Click **More > Edit** next to the pipeline name.

Figure 10-125 Entry for editing a pipeline



Step 7 On the **Edit Pipeline** page, set pipeline parameters. For details about the parameters, see [Table 10-59](#).

Table 10-59 Editing a pipeline

Parameter	Description
Data Spaces	Data space to which the pipeline belongs. This parameter cannot be modified.
Pipeline Name	Name you specified for the pipeline. The name cannot be changed after the pipeline is created.
Shards	The number of shards of the pipeline. The value range is 1 to 64.
Lifecycle	Life cycle of data in the pipeline. Value range: 7-180
Description	Remarks on the pipeline. This parameter is optional.

Step 8 Click **OK**.

----End

10.5.10.4 Deleting a Pipeline


Data in the pipeline will also be deleted and cannot be restored. Exercise caution when performing this operation.

Limitations and Constraints

Pipelines created by the system cannot be deleted.

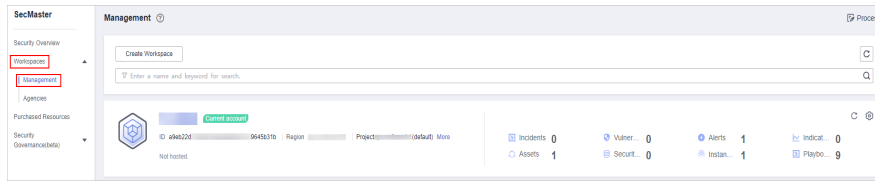
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

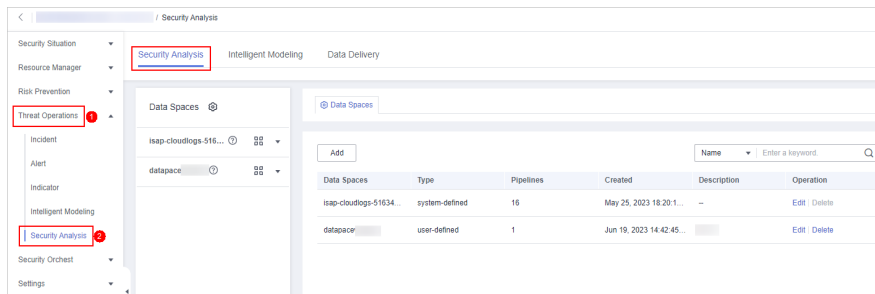
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-126 Management



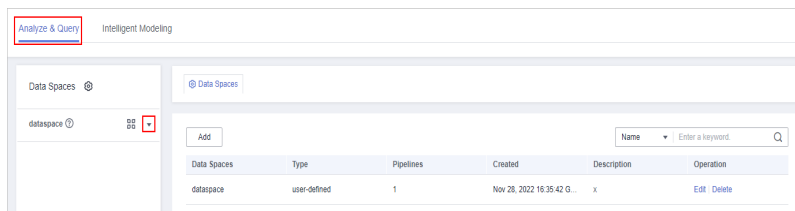
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-127 Accessing the Security Analysis tab page



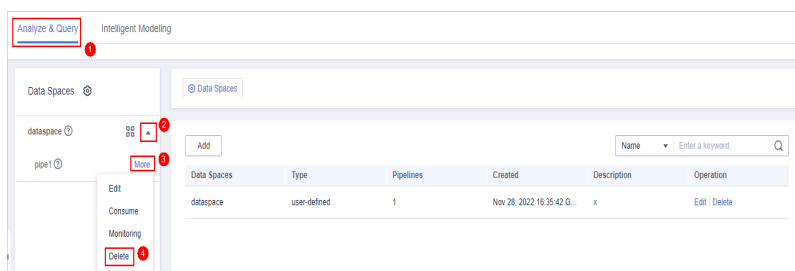
Step 5 In the data space navigation tree on the left, click the data space name or **▼** to view the created pipeline.

Figure 10-128 Viewing pipeline details



Step 6 Click **More > Delete** next to the pipeline name.

Figure 10-129 Deleting a pipeline



Step 7 In the dialog box that is displayed, click **OK**.

----End

10.6 Data Consumption

Data consumption refers to the process during which third-party software or cloud products consume the log data in real time through a client. It is a sequential read/write from/into full data.

SecMaster provides the data consumption function and supports real-time data consumption through the client.

Enabling Data Consumption


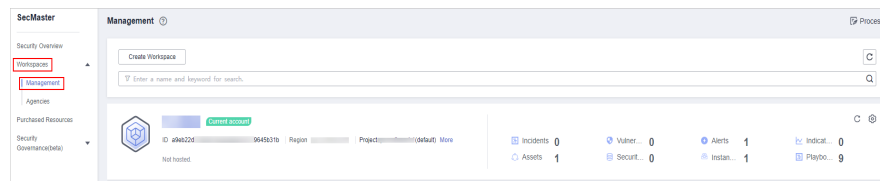
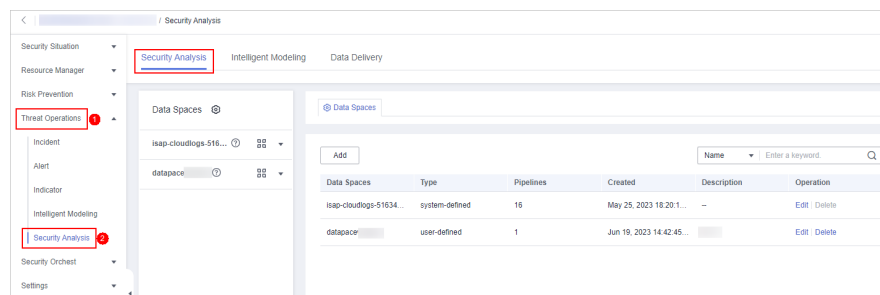
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-130 Management



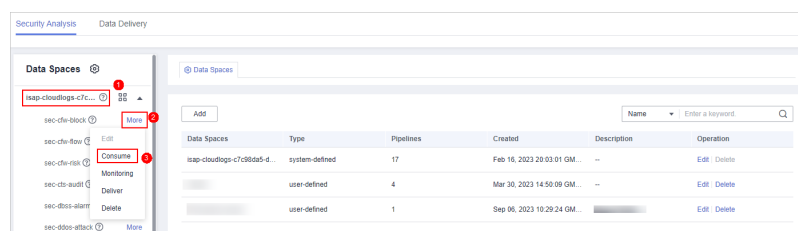
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-131 Accessing the Security Analysis tab page



- Step 5** In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More > Consume**.

Figure 10-132 Accessing the data consumption page



Step 6 On the Data Consumption page, click  next to Current Status to enable data consumption.


After the function is enabled, the consumption configuration information is displayed, as shown in [Table 10-60](#).

Table 10-60 Data consumption parameters

Parameter	Description
Status	Status of the data consumption function in the current pipeline
Pipeline Name	Name of the current pipeline
Subscriber	The preset subscription mode in the system, which determines how data is transmitted to consumers.
Access Node	Access node of the current data.

----End

Related Operations

After data consumption is enabled, you can click  next to **Status** on the Data Consumption page to disable data consumption.

10.7 Data Delivery

10.7.1 Creating a Data Delivery

SecMaster can deliver data to other pipelines or other products in real time so that you can store data or consume data with other systems. After data delivery is configured, SecMaster periodically delivers the collected data to the specified pipelines or cloud products.

Currently, data can be delivered to the following cloud products: Object Storage Service (OBS) and Log Tank Service (LTS).

Prerequisites

- To deliver data to OBS, ensure there is an available bucket whose bucket policy is **Public Read and Write**.
- To deliver data to LTS, ensure there is an available log group and log streams.

Limitations and Constraints

When performing cross-account delivery, the data can only be delivered to the pipelines instead of cloud services of other accounts.

Creating a Data Delivery


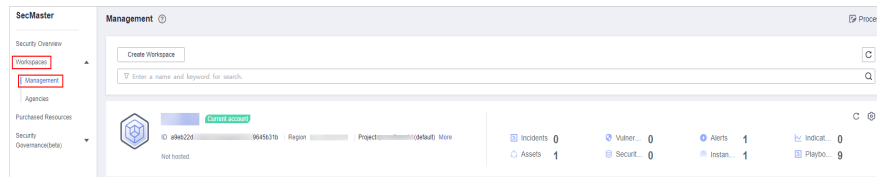
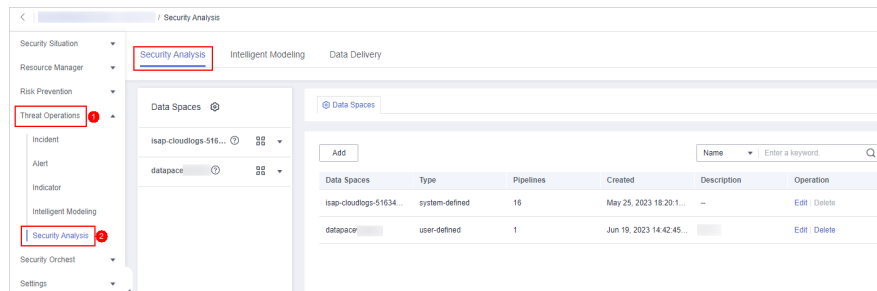
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-133 Management



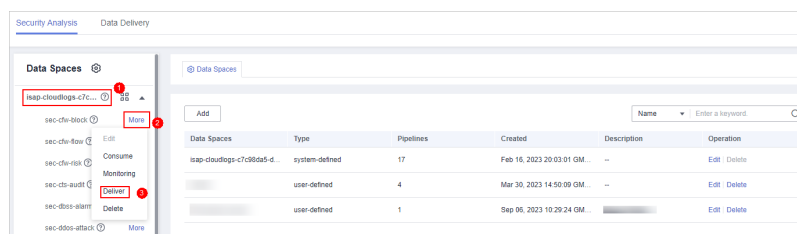
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-134 Accessing the Security Analysis tab page



- Step 5** In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More > Deliver**.

Figure 10-135 Accessing data delivery settings page



- Step 6** (Optional) Authorization of the destination type is required for the first delivery. If the authorization has been performed, skip this step.

Confirm the authorization information, select **Agree to authorize** and click **OK**.

- Step 7** On the **Create Delivery** page, set data delivery parameters.

1. Configure basic information.

Table 10-61 Basic information

Parameter	Description
Delivery Name	Customized delivery rule name
Resource Consumption	The value is generated by default and does not need to be configured .

2. Configure the data source.

In the **Data Source Settings** area, the detailed information about the current pipeline is displayed. **You do not need to set this parameter.**

Table 10-62 Data source parameters

Parameter	Description
Delivery Type	Delivery destination type. The default value is PIPE .
Region	Area where the current pipeline is located
Workspace	Workspace to which the current pipeline belongs
Data Spaces	Data space to which the current pipeline belongs
Pipeline	Pipeline name
Data Read Policy	Data read policy of the current pipeline
Read By	Identity of the data source reader

3. Configure the delivery destination.

- **PIPE**: Deliver the current pipeline data to other pipelines of the current account or pipelines of other accounts. Set this parameter as required.
 - **Current**: Deliver the current pipeline data to another pipeline of the current account. For details about the parameters, see [Table 10-63](#).

Table 10-63 Destination parameters - PIPE of the current account

Parameter	Description
Account Type	Account type of the data delivery destination. Select Current .
Delivery Type	Delivery type. Select PIPE .
Workspace	Workspace where the destination PIPE is located
Data Spaces	Data space where the destination PIPE is located
Pipeline	Pipeline where the destination PIPE is located

Parameter	Description
Written To	The value is generated by default and does not need to be configured.

- Cross-account delivery: Deliver the current pipeline data to the pipeline of another account. For details about the parameters, see [Table 10-64](#).

Table 10-64 Destination parameters - PIPE

Parameter	Description
Account Type	Account type of the data delivery destination. Select Other .
Delivery Type	Delivery type. Select PIPE .
Account ID	ID of the account to which the destination PIPE belongs
Workspace ID	ID of the workspace where the destination PIPE is located. For details about how to query the workspace ID, see Step 6 .
Data Space ID	ID of the data space where the destination PIPE is located. For details about how to query the data space ID, see Step 6 .
Pipeline ID	ID of the pipeline where the destination PIPE is located. For details about how to query the pipeline ID, see Step 6 .
Written To	The value is generated by default and does not need to be configured.

- **LTS**: Deliver the pipeline data to LTS. For details about the parameter settings, see [Table 10-65](#).

To deliver data to LTS, ensure there is an available log group and log streams.

Table 10-65 Destination parameters - LTS

Parameter	Description
Account Type	Account type of the data delivery destination. When delivering data to LTS, only the current account type can be selected.
Delivery Type	Delivery type. Select LTS .
Log Group	Destination LTS log group

Parameter	Description
Log Stream	Destination LTS log stream
Written To	The value is generated by default and does not need to be configured.

- **OBS:** Deliver the pipeline data to OBS. For details about the parameter settings, see [Table 10-66](#).

To deliver data to OBS, ensure there is an available bucket whose bucket policy is **Public Read and Write**.

Table 10-66 Destination parameters - OBS

Parameter	Description
Account Type	Account type of the data delivery destination. When delivering data to OBS, only the current account type can be selected.
Delivery Type	Delivery type. Select OBS .
Bucket Name	Name of the destination OBS bucket
Written To	The value is generated by default and does not need to be configured.

Step 8 Click **OK**.

----End

Follow-up Operation

After a data delivery task is added, you need to grant the delivery permission. The delivery takes effect only after you accept the authorization. For details, see [Data Delivery Authorization](#).

10.7.2 Data Delivery Authorization

After a data delivery is added, you need to grant the delivery permission. The delivery takes effect only after the permission is granted.

Prerequisites

Data delivery has been added.

Limitations and Constraints

If the new data delivery is a cross-account delivery, you need to log in to the destination account to perform authorization.

Procedure


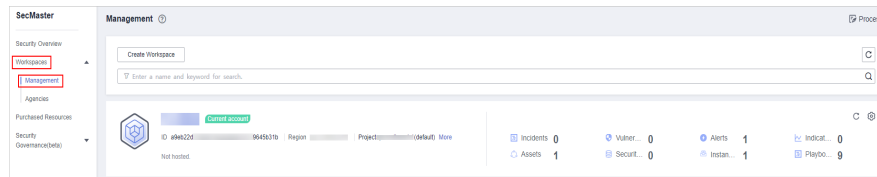
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

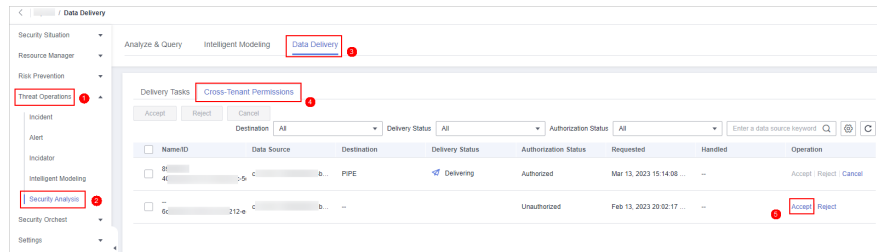
Figure 10-136 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. On the **Security Analysis** page that is displayed, click the **Data Delivery** tab. The **Data Delivery** page is displayed.
- Step 5** On the **Data Delivery** page, click the **Cross-tenant Permissions** tab. On the page that is displayed, click **Accept** in the **Operation** column of the target delivery task.

To accept authorization in batches, select all tasks to be authorized and click **Accept** in the upper left corner of the list.

Figure 10-137 Authorization for data delivery



After the authorization is granted, the authorization status of the target delivery task is updated to **Authorized**. You can go to the delivery destination to view the delivery details. For details, see [Checking the Data Delivery Status](#).

----End

Related Operations

On the **Cross-tenant Permissions** tab page, you can select to **Reject** or **Cancel** the authorization.

Table 10-67 Cross-tenant permission authorization options

Operation	Description
Reject	In the row containing the target delivery task, click Reject in the Operation column to reject the authorization. To reject authorization in batches, select all tasks to be rejected and click Reject in the upper left corner of the list.
Cancel	1. In the row containing the target delivery task, click Cancel in the Operation column to cancel the authorization. To cancel authorization in batches, select all tasks to be canceled and click Cancel in the upper left corner of the list. 2. In the displayed dialog box, click OK .

10.7.3 Checking the Data Delivery Status

After the data is successfully delivered, you can view the data delivery status at the delivery destination. You can also perform the following operations:


- [Delivering to Other Pipelines](#)
- [Delivering to OBS Bucket](#)
- [Delivering to LTS](#)

Prerequisites

Data has been delivered. For details, see [Creating a Data Delivery](#).

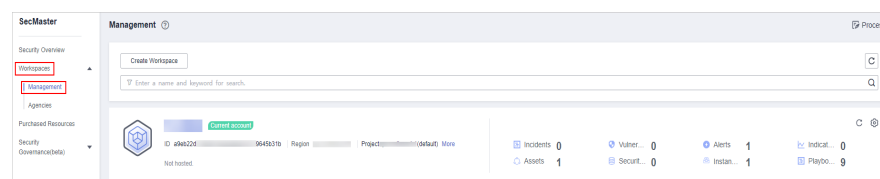
Delivering to Other Pipelines

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

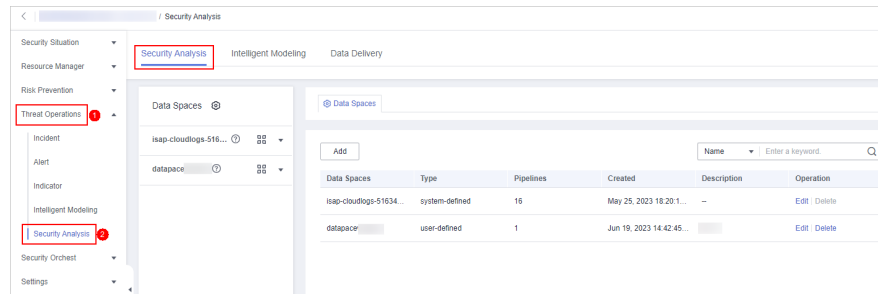
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-138 Management



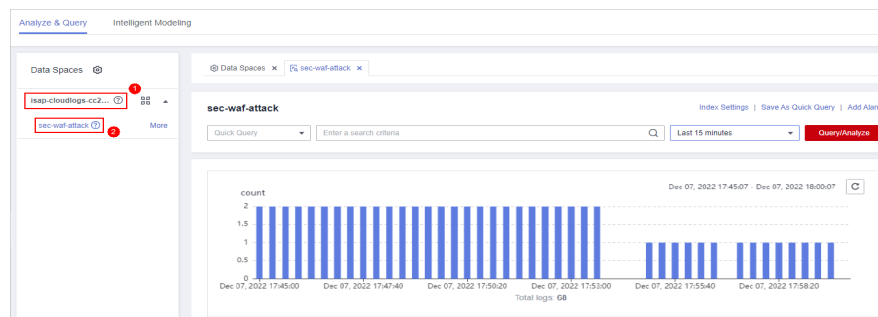
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-139 Accessing the Security Analysis tab page



Step 5 In the data space navigation tree on the left, click a data space name to show the pipeline list. Click a pipeline name. On the displayed page, you can search the pipeline data.

Figure 10-140 Pipeline data page




Step 6 In the target pipeline, view the delivery log information.

----End

Delivering to OBS Bucket

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Storage > Object Storage Service**. The bucket list page is displayed.


Step 3 On the bucket list page, click the name of the OBS bucket selected for data delivery. The details page of the target OBS bucket is displayed.


Step 4 On the OBS bucket details page, view the delivery log information.

----End

Delivering to LTS

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance > Log Tank Service**.

Step 3 In the log group list on the **Log Management** page, locate the log group for which you want to add data delivery and click  before to the log group name.

Step 4 Click the name of the log stream selected during data delivery. The log stream details page is displayed.

Step 5 On the log stream details page, view the delivered log information.

----End

10.7.4 Managing Data Delivery

This section describes how to manage delivery tasks.


- [Viewing a Data Delivery Task](#)
- [Suspending a Delivery Task](#)
- [Starting a Delivery Task](#)
- [Deleting a Delivery Task](#)

Prerequisites

A data delivery task has been added.

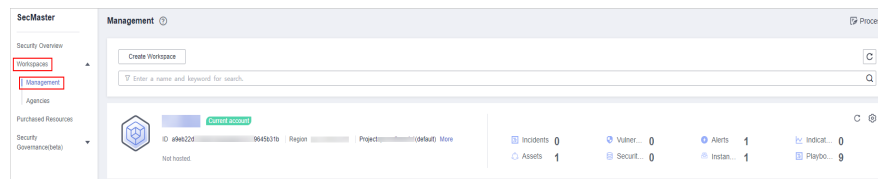
Viewing a Data Delivery Task

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

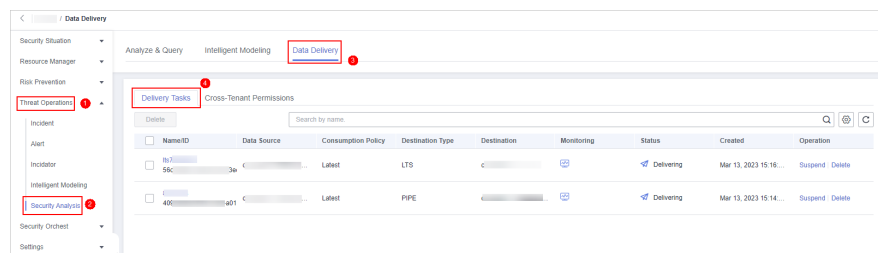
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-141 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.

Figure 10-142 Data Delivery tab page



Step 5 On the delivery task list page, view existing delivery tasks.

Table 10-68 Delivery task parameters

Parameter	Description
Name/ID	Delivery task name and ID
Data Source	Pipeline where the data source is located
Consumption Policy	Consumption policy of a delivery task
Destination Type	Type of the data delivery destination
Destination	Data delivery destination
Monitoring	Data delivery monitoring status. You can click the monitoring icon to view the data consumption information.
Status	Status of a delivery task
Created	Time when a delivery task is created
Operation	You can delete or suspend a data delivery task.

----End

Suspending a Delivery Task

After a data delivery task is added and authorized, the delivery task status changes to **Delivering**. To stop the delivery, you can suspend the target delivery task.


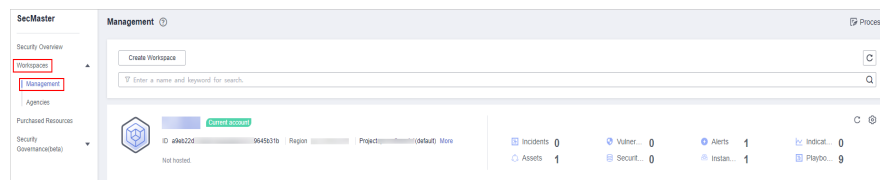
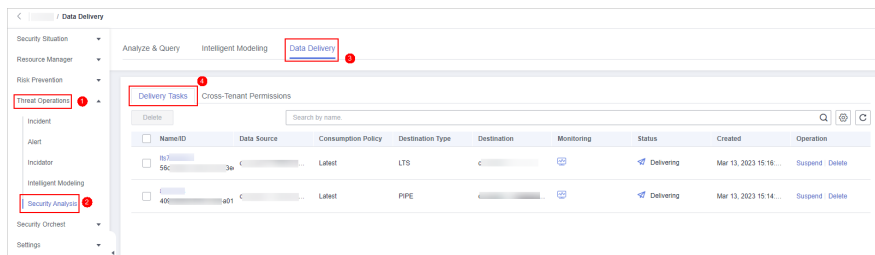
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-143 Management



- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.

Figure 10-144 Data Delivery tab page



Step 5 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Suspend** in the **Operation** column.


After a delivery task is suspended, the delivery task status changes to **Suspended**, indicating that the delivery task is suspended successfully.

----End

Starting a Delivery Task

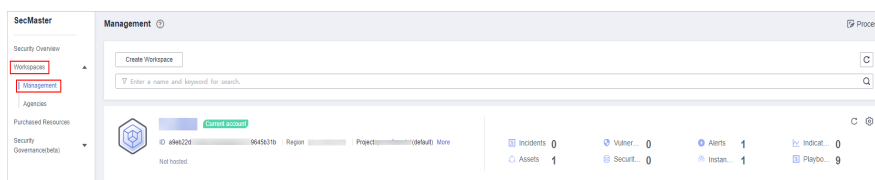
You can restart a suspended delivery task.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

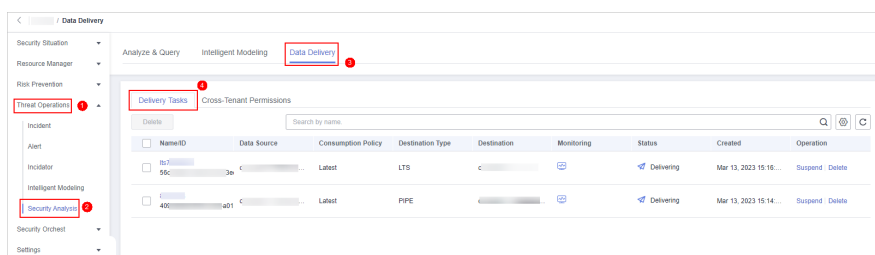
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-145 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.

Figure 10-146 Data Delivery tab page



Step 5 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Start** in the **Operation** column.


After a delivery task is restarted, the delivery task status changes to **Delivering**, indicating that the delivery task is successfully started.

----End

Deleting a Delivery Task

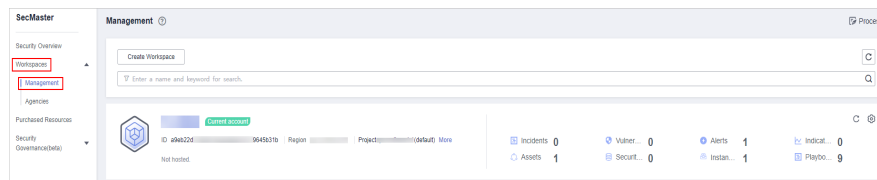
If a data delivery task is no longer needed, you can delete it.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

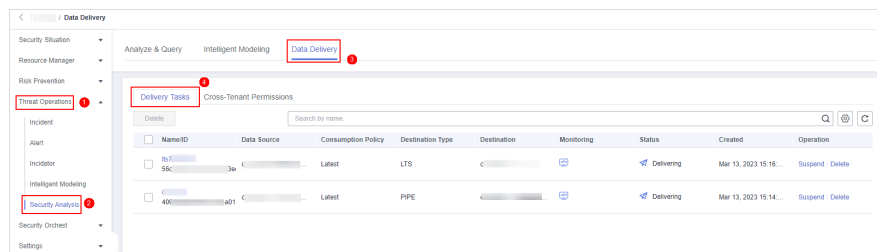
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-147 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.

Figure 10-148 Data Delivery tab page



Step 5 On the **Data Delivery** tab page, locate the row of the target delivery task and click **Delete** in the **Operation** column and click **OK** in the displayed dialog box.

----End

10.8 Data Monitoring

SecMaster can monitor metrics such as the production rate, production volume, and total consumption rate of the upstream and downstream SecMaster pipelines. You can check the service status based on the monitoring results.


Basic Concepts

- A producer is a logical object used to construct data and transmit it to the server. It stores data in message queues.

- A subscriber is used to subscribe to SecMaster pipeline messages. A pipeline can be subscribed to by multiple subscribers. SecMaster distributes messages through subscribers.
- A consumer is a running entity that receives and processes data. It consumes and processes messages in the SecMaster pipeline through subscribers.
- A message queue is the container for data storage and transmission.

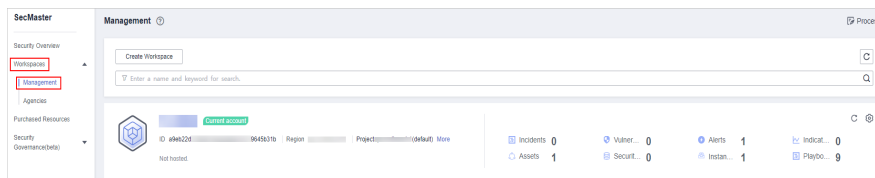
Viewing Metrics

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

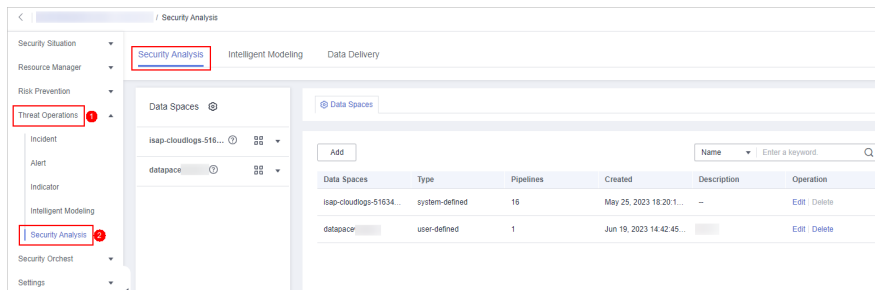
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 10-149 Management



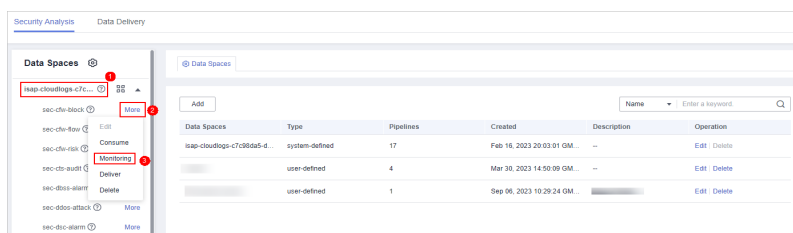
Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

Figure 10-150 Accessing the Security Analysis tab page



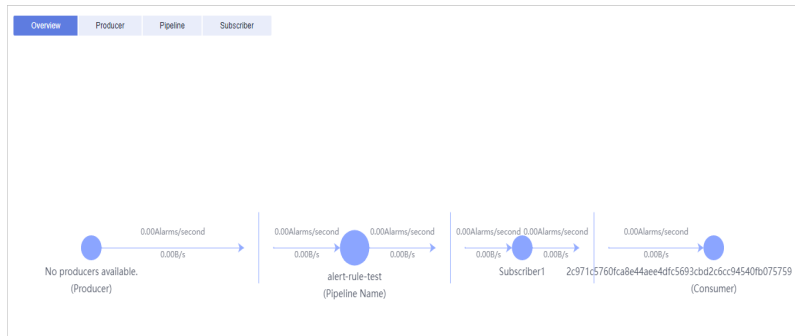
Step 5 In the data space navigation tree on the left, click the data space name to expand all pipelines. Next to the name of the target pipeline, click **More > Monitoring**.

Figure 10-151 Data monitoring page



Step 6 On the pipeline monitoring page, view monitoring metrics.

Figure 10-152 Viewing monitored data



- **Overview:** Displays information such as the production rate between producers, pipelines, subscribers, and consumers in the current pipeline.
- **Producer:** Displays metrics of the producer, such as current production TPS, current production rate, current production volume, and current message storage size.
- **Pipeline:** Displays the pipeline message size (MB), producer-to-pipeline message size (MB), producer-to-pipeline messages, message size consumed by pipelines (MB), messages consumed by pipelines, unacknowledged message size (MB), pipeline production rate, pipeline consumption rate, average message size (KB), and offloaded message size (B) in a specified period (last 2/6/12/24 hours, last 7 days, or a customized period).
- **Subscriber:** displays the total consumption rate of subscribers, consumed data volume (B), consumed messages, and active consumers in a specified period (last 2/6/12/24 hours, last 7 days, or a user-defined period).

----End

11 Security Orchestration

11.1 Security Orchestration Overview

Security orchestration combines security functions of different systems or components in a system involved in security operations of enterprises and organizations based on certain logical relationships to complete a specific security operations process and procedure. It aims to help security teams of enterprises and organizations quickly and efficiently respond to network threats and implement efficient and automatic response and handling of security incidents.

It provides the following functions:

- **Playbook management:** you can use the built-in automatic response playbooks or customize playbooks.
- **Workflow:** Allows you to draw a playbook triggering flowchart.
- **Instance management:** allows you to monitor and manage running instances and view records.
- **SOAR:** You can orchestrate workflows to let SOC automatically handle security incidents and suspicious incidents.

Basic Concepts

- **Playbook**

A playbook is a formal expression of the security operation workflow in the security orchestration system and is usually executed driven by the workflow engine in the orchestrator.

Orchestrating a playbook is to build the manual security operation workflow and software into a machine playbook.

- **Workflow**

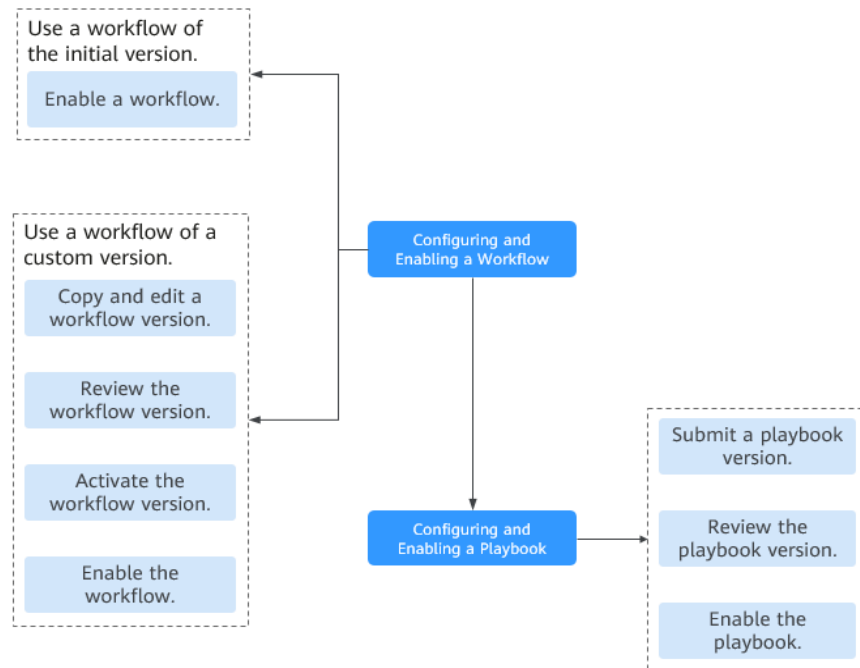
A workflow is a collaborative work mode that integrates various capabilities related to security operation, such as tools, technologies, workflows, and personnel. A workflow is the response flow when a playbook is triggered.

It combines API-enabled security capabilities, or applications, in SecMaster and manual checkpoints based on certain logical relationships to complete a specific security operations process and procedure.

11.2 Security Orchestration Process

This topic describes how Security Orchestration works.

Figure 11-1 Security orchestration flowchart



1. **Configuring and Enabling a Workflow:** Enables the required built-in workflow of SecMaster.
By default, SecMaster provides workflows such as WAF uncapping, Synchronization of HSS alert status, and Fetching indicator from alert. The initial version (V1) of the workflows has been activated. You only need to enable the workflows and use them in playbooks.
In addition, if you need to edit a workflow, you can copy the initial version for processing.
2. **Configuring and Enabling a Playbook:** Enables the required built-in playbook of SecMaster.
By default, SecMaster provides playbooks such as Fetching indicator from alert, Synchronization of HSS alert status, and Automatic closing of repeated alerts. To use a playbook, you need to enable it.
A playbook supports multiple versions. You need to submit the required playbook version for review before enabling the playbook.

11.3 Configuring and Enabling a Workflow

By default, SecMaster provides workflows such as WAF uncapping, Synchronization of HSS alert status, and Fetching indicator from alert. The initial version (V1) of the workflows has been activated. To use the initial version of a workflow, you only need to enable the workflow.


You can customize and edit existing workflows.

This section describes how to configure and enable a workflow.

- [Enabling a Workflow of the Initial Version](#)
- [Enabling a Workflow of a Custom Version](#)

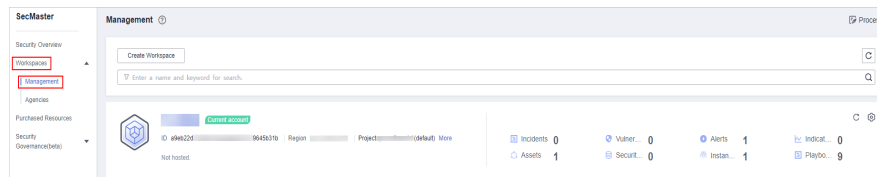
Enabling a Workflow of the Initial Version

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

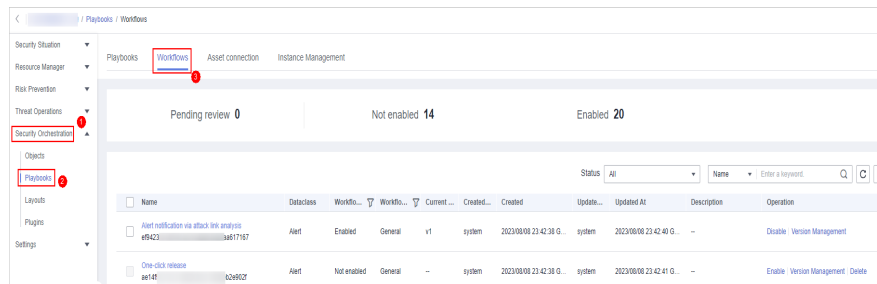
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-2 Management



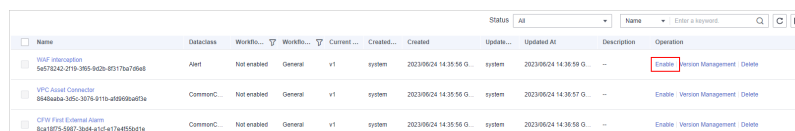
Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-3 Workflows tab page



Step 5 Locate the row containing your desired workflow and click **Enable** in the **Operation** column.

Figure 11-4 Enabling a workflow



Step 6 On the slide-out panel displayed, select the workflow version to be enabled and click **OK**.

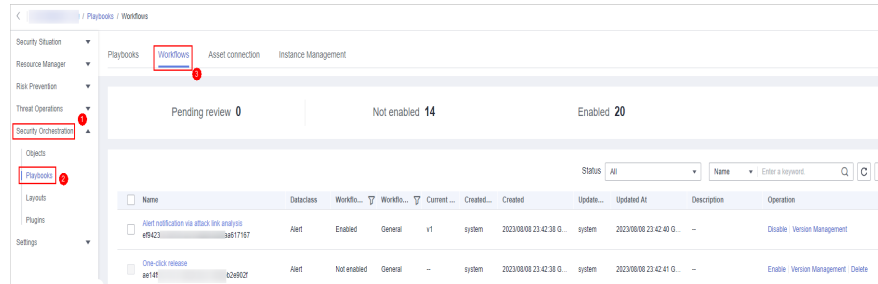
----End

Enabling a Workflow of a Custom Version

Accessing the workflow management page

Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

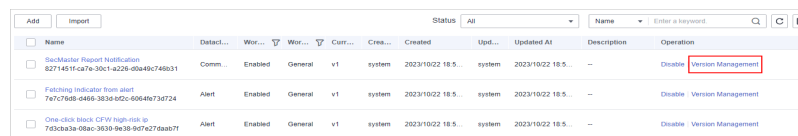
Figure 11-5 Workflows tab page



Copying a workflow version

Step 2 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-6 Version Management page



Step 3 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Copy** in the **Operation** column.

Step 4 In the dialog box displayed, click **OK**.

Editing and submitting a workflow version

Step 5 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Edit** in the **Operation** column.

Step 6 On the workflow drawing page, drag basic, workflow, and plug-in nodes from **Resource Libraries** on the left to the canvas on the right for workflow design.

Table 11-1 Resource Libraries parameters

Parameter		Description	
Basic	Basic Node	StartEvent	The start of a workflow. Each workflow can have only one start node. The entire workflow starts from the start node.
		EndEvent	The end of a workflow. Each workflow can have multiple end nodes, but the workflow must end with an end node.

Parameter		Description	
	UserTask	When the workflow execution reaches this node, the workflow is suspended and a to-do task is generated on the Task Center page. After you complete the task, the subsequent nodes in the workflow continue to be executed. Table 11-2 describes the UserTask parameters.	
	SubProcess	Another workflow is started to perform cyclic operations. It is equivalent to the loop body in the workflow.	
	System Gateway	ExclusiveGateway	During line distribution, one of the multiple lines is selected for execution based on the condition expression. During line aggregation, if one of the multiple lines arrives, the subsequent nodes continue to execute the task.
		ParallelGateway	During line distribution, all lines are executed. During line aggregation, the subsequent nodes are executed only when all the lines arrive. (If one line fails, the entire workflow fails.)
		InclusiveGateway	During line distribution, all expressions that meet the conditions are selected for execution based on the condition expression. During line aggregation, subsequent nodes are executed only when all lines executed during traffic distribution reach the inclusive gateway. (If one line fails, the entire workflow fails.)
Workflows		You can select all released workflows in the current workspace.	
Plug-ins		You can select all plug-ins in the current workspace.	

Table 11-2 UserTask parameters

Parameter	Description
Primary key ID	The system automatically generates a primary key ID, which can be changed as required.
Workspace Name	Name of the manual review node
Expired	Expiration time of a manual review node
Description	Description of the manual review node

Parameter	Description
View Parameters	Click >> . On the Select Context page that is displayed, select an existing parameter name. To add a parameter, click Add Parameter .
Manual Handling Parameters	Key of the input parameter To add a parameter, click Add Parameter .
Processed By	Set the reviewer of the workflow to the IAM user of the current account. If a workflow needs to be approved after the setting, only the owner can handle it on the Task Center page. Non-owners can only view the workflow. NOTE In first time use, you need to obtain authorization. Detailed operations are as follows: 1. Click Authorize . 2. On the Access Authorization slide-out panel displayed, select Agree and click OK .

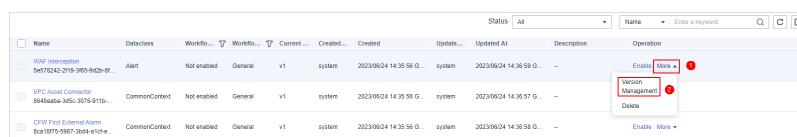
Step 7 After the design is complete, click **Save and Submit** in the upper right corner. In the automatic workflow verification dialog box displayed, click **OK**.

If the workflow verification fails, check the workflow based on the failure message.

Reviewing a workflow version

Step 8 After the workflow version is edited and submitted, the workflow management page is displayed. On the workflow management page, click **Version Management** in the **Operation** column of the target workflow.

Figure 11-7 Version Management page



Step 9 On the **Version Management** slide-out panel, click **Review** in the **Operation** column of the target workflow.

Step 10 In the review confirmation dialog box, set **Review Comment** to **Pass** and click **OK**.

Activating a workflow version

Step 11 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Activate** in the **Operation** column.

Step 12 In the dialog box displayed, click **OK**.

Enabling a workflow

- Step 13** On the **Version Management** slide-out panel, click **Enable** in the **Operation** column of the target workflow.
 - Step 14** On the slide-out panel displayed, select the workflow version to be enabled and click **OK**.
- End

11.4 Configuring and Enabling a Playbook

By default, SecMaster provides playbooks such as Fetching indicator from alert, Synchronization of HSS alert status, and Synchronization of HSS alert status. To use a playbook, you need to enable it.

This section describes how to configure and enable a playbook.

Prerequisites

A workflow has been enabled by referring to [Configuring and Enabling a Workflow](#).

Step 1: Submitting a Playbook Version


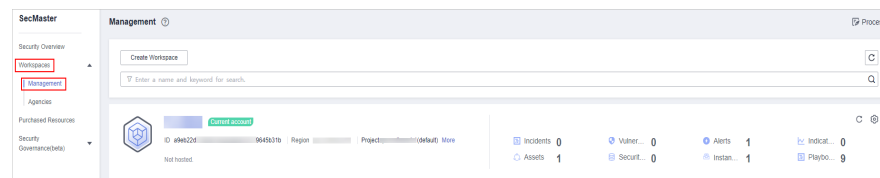
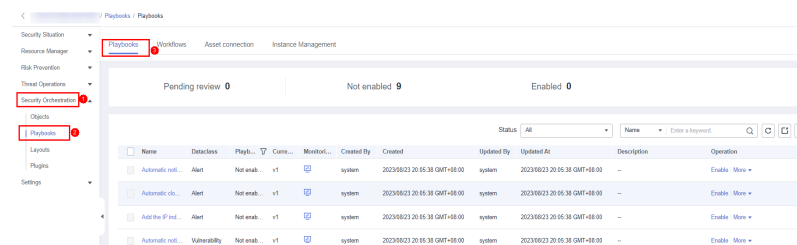
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-8 Management



- Step 4** In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-9 Accessing the Playbooks tab



- Step 5** In the **Operation** column of the target playbook, click **Versions**.
- Step 6** On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Submit** in the **Operation** column.

Step 7 In the confirmation dialog box, click **OK** to submit the playbook version.

 **NOTE**

- After the playbook version is submitted, **Version Status** changes to **To be reviewed**.
- After a playbook version is submitted, it cannot be edited. To edit it, create a version or reject it during review.

----End

Step 2: Reviewing the Playbook Version

Step 1 In the **Operation** column of the target playbook, click **Versions**.

Step 2 On the version management page, click **Review**.

Step 3 On the **Review Playbook Version** page, enter the review information. [Table 11-3](#) describes the parameters for reviewing a playbook version.

Table 11-3 Parameters for reviewing a playbook version

Parameter	Description
Comments	Select the review conclusion. <ul style="list-style-type: none"> • If the playbook version is approved, the status of the playbook version changes to Activated. • After the playbook version is rejected, the status of the playbook version changes to Rejected. You can edit the playbook version and submit it again.
Reason for Rejection	This parameter is mandatory when Comments is Reject . Enter the review comment. This parameter is mandatory when Reject is selected for Comments .

 **NOTE**

If there is only one version available for the current playbook, the version is in the **Activated** state by default after being approved.

Step 4 Click **OK** to complete the playbook version review.

----End

Step 3: Enabling the Playbook

Step 1 On the **Version Management** slide-out panel, click **Enable** in the **Operation** column of the target playbook.

Step 2 After selecting the playbook version to be enabled, click **OK**.

----End

11.5 Operation Object Management

11.5.1 Data Class

11.5.1.1 Viewing Data Classes

The playbook and workflow running in security orchestration and response need to be bound to a data class. The playbook is triggered by a data object (instance of the data class).

Procedure


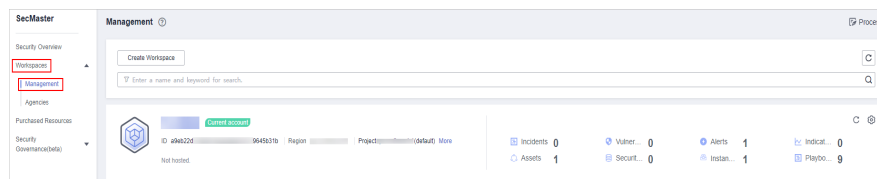
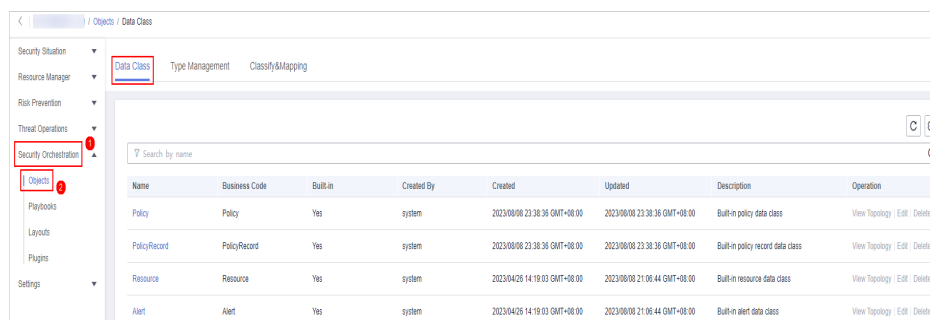
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-10 Management



- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. The **Data Class** tab page is displayed by default.

Figure 11-11 Accessing the Data Class tab



- Step 5** In the data class list, view the existing data class information.


If there are a large number of data classes, you can select the data class name, code, built-in or not, or description, enter a keyword in the search box, and click  to quickly search for a specified data class.

Table 11-4 Data Information

Parameter	Description
Name	Name of a data class.
Business Code	Business code of the data type.
Built-in	Indicates whether the data class is a built-in data class.
Created By	Creator information of the data class.
Created	Time when a dataset is created.
Updated	Time when a dataset is updated.
Description	Description of a data class
Operation	You can edit and delete data classes.

Step 6 To view details about a data class, click the name of the target data class. The details page of the target data class is displayed on the right.

----End

11.5.2 Type Management

11.5.2.1 Managing Alert Types

This section describes how to manage alert types. The detailed operations are as follows:

- **Viewing Alert Types:** describes how to view existing alert types and their details.
- **Adding an Alert Type:** describes how to create custom alert types.
- **Associating an Alert Type with a Layout:** describes how to associate a custom alert type with an existing layout.
- **Editing an Alert Type:** describes how to edit a custom alert type.
- **Managing an Alert Type:** describes how to enable, disable, and delete a custom alert type.

Limitations and Constraints

- By default, built-in alert types are associated with existing layouts. You **cannot** customize associated layouts.
- Built-in alert types are enabled by default and **cannot** be edited, disabled, or deleted.
- After a customized alert type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

Viewing Alert Types


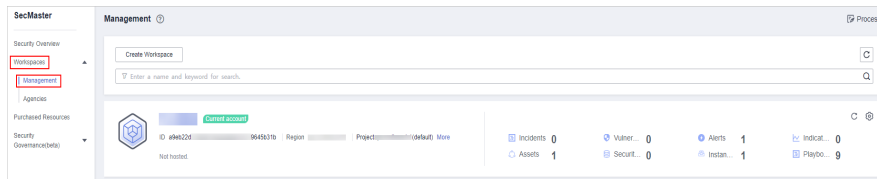
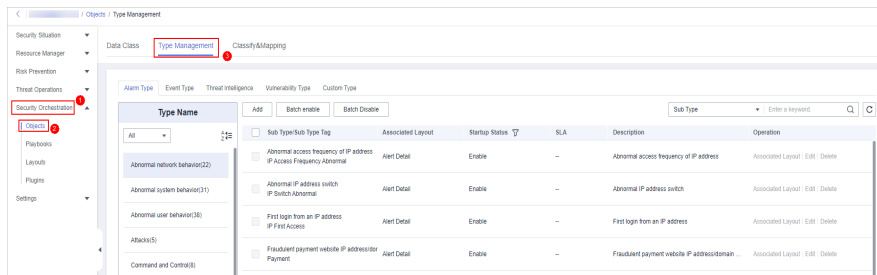
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-12 Management



- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-13 Type Management page



- Step 5** On the **Type Management** page, click the **Alarm Type** tab.
- Step 6** On the **Alarm Type** tab page, you can view all alert types in the **Type Name** area on the left.

To view details about subtypes of an alert type, click the target type name in **Type Name** on the left. Details about all subtypes are displayed on the right. For details about the parameters, see [Table 11-5](#).

If there are many subtypes, you can select the **Sub Type** or **Associated Layout** and enter the corresponding keyword for search.

Figure 11-14 Viewing alert types

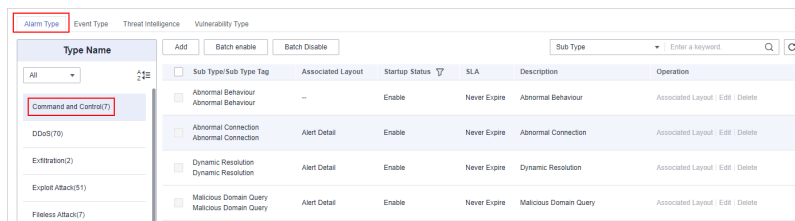


Table 11-5 Alert type parameters

Parameter	Description
Sub Type/Sub Type Tag	Name and ID of an alert subtype.
Associated Layout	Layout associated with the alert type.
Startup Status	Whether an alert type is enabled <ul style="list-style-type: none"> ● Enabled: The current type has been enabled. ● Disabled: The current type has been disabled.
SLA	SLA processing time of an alert type.
Description	Description of an alert type
Operation	You can edit and delete alert or incident types.

----End

Adding an Alert Type


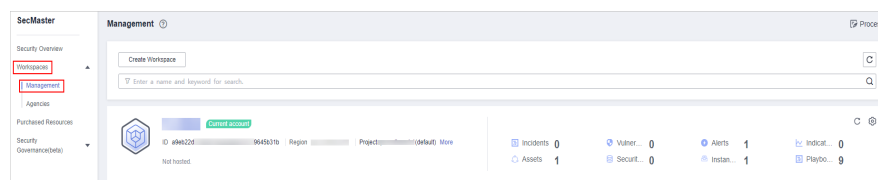
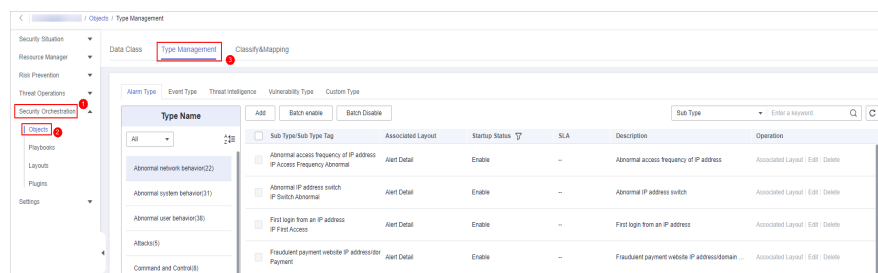
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-15 Management



- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.



Figure 11-16 Type Management page



- Step 5** On the **Type Management** page, click the **Alarm Type** tab.

Step 6 On the **Alarm Type** page, click **Add**. On the **Add Alarm Type** slide-out panel, set alert type parameters.

Table 11-6 Parameters for adding an alert type

Parameter	Description
Type Name	Customize the name of the new alert type. The name must comply with the upper camel case naming rules, for example, TypeName .
Type Tag	Enter the alert type ID. The keyword must comply with the upper camel case naming rules, for example, TypeTag .
Sub Type	Enter the subtype of the alert type. The name must comply with the upper camel case naming rules, for example, SubType .
Sub Type Tag	Enter the alert subtype ID. The keyword must comply with the upper camel case naming rules, for example, SubTypeName .
Startup Status	Indicates whether an alert type is enabled. <ul style="list-style-type: none">  : indicates that the alert type is enabled.  : indicates that the type is disabled.
SLA	Set the SLA processing time of the alert.
Description	Description of a user-defined alert type

 **NOTE**

After a customized alert type is added, the **Type Name**, **Type Tag**, and **Sub Type Tag** parameters cannot be modified.

Step 7 In the lower right corner of the page, click **OK**.

After the alert type is added, you can view the new alert type in **Type Name** area on the **Alarm Type** page.


----End

Associating an Alert Type with a Layout

 **NOTE**

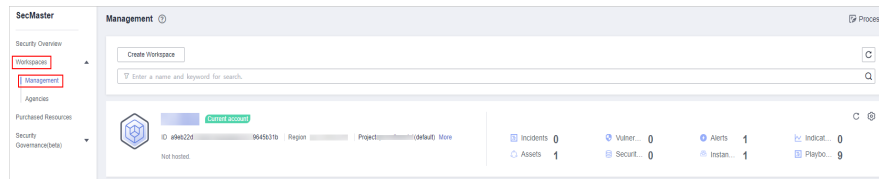
By default, built-in alert types are associated with existing layouts. You cannot customize associated layouts.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

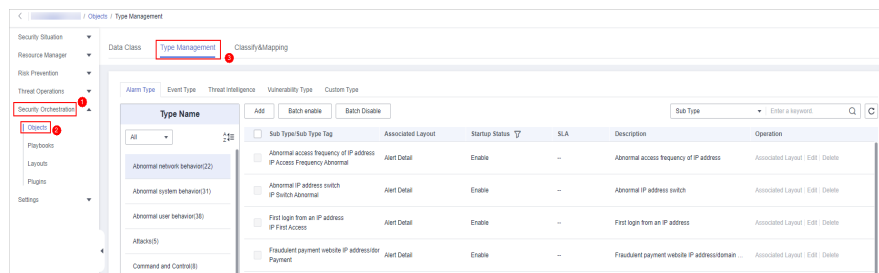
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-17 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-18 Type Management page



Step 5 On the **Type Management** page, click the **Alarm Type** tab.

Step 6 On the type management page, select the type to be associated with a layout and click **Associated Layout** in the **Operation** column of the target type.

Step 7 In the **Associate Layout** dialog box, select the layout to be associated.

Step 8 Click **OK**.


----End

Editing an Alert Type

NOTE

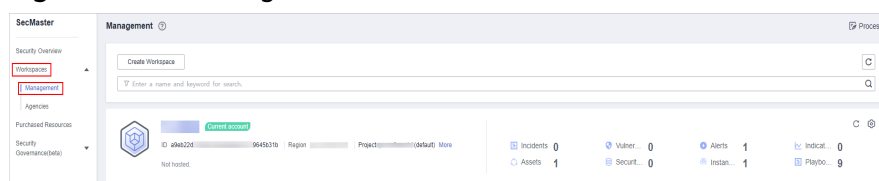
- Currently, the built-in alert type cannot be edited.
- After a customized alert type is added, the **Type Name**, **Type Tag**, and **Sub Type Tag** parameters cannot be modified.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

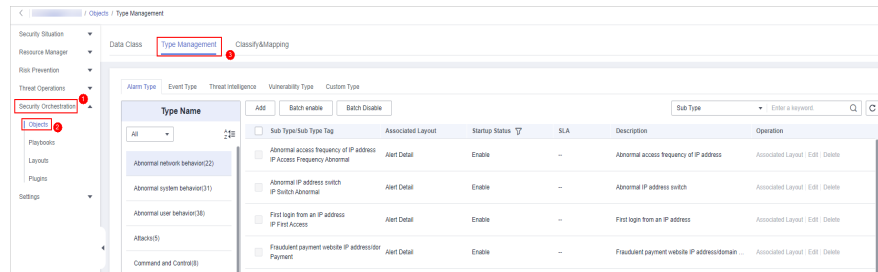
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-19 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-20 Type Management page





Step 5 On the **Type Management** page, click the **Alarm Type** tab.

Step 6 In **Type Name** on the **Alarm Type** page, click the name of the custom alert type to be edited. Details about the custom alert type are displayed on the right.

Step 7 On the alert list page on the right, locate the row that contains the target type and click **Edit** in the **Operation** column.

Step 8 On the displayed page, modify the parameters of the alert type.

Table 11-7 Parameters for editing an alert type


Parameter	Description
Type Name	Name of an alert type, which cannot be modified.
Type ID	Alert type ID, which cannot be modified.
Sub Type	Enter the subtype of the alert type.
Sub Type Tag	Alert subtype ID, which cannot be modified.
Status	Sets the startup status of an alert type. <ul style="list-style-type: none"> ●  : indicates that the type is enabled. ●  : indicates that the type is disabled.
SLA	Set the SLA processing time of the alert.
Description	Description of a custom alert type

Step 9 In the lower right corner of the page, click **OK**.

----End

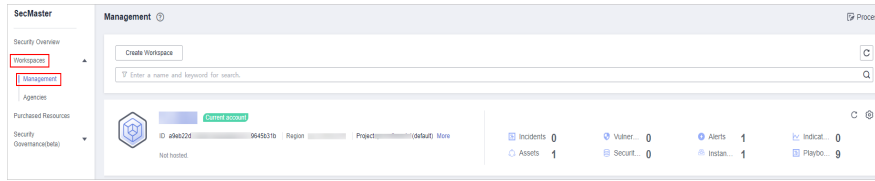
Managing an Alert Type

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

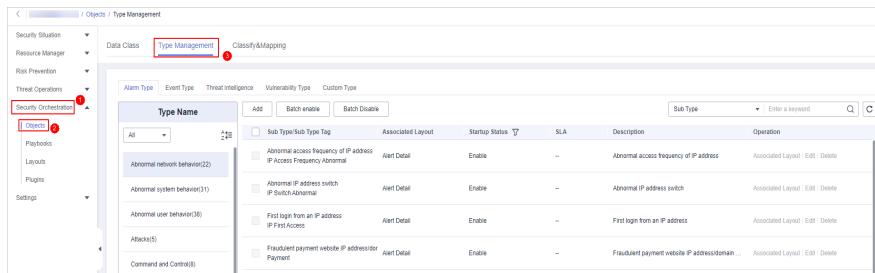
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-21 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-22 Type Management page



Step 5 On the **Type Management** page, click the **Alarm Type** tab.

Step 6 On the alert type tab, manage alert types.

Table 11-8 Managing an alert type

Parameter	Description
<p>Enable</p> <p>NOTE The built-in alert types are enabled by default. You do not need to manually enable them.</p>	<ol style="list-style-type: none"> On the Alarm Type page, select the types to be enabled and click Batch enable. Alternatively, locate the row containing the alert type to be enabled, click Disable in the Status column. In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the status of the target type changes to Enable, the target type is enabled successfully.
<p>Disable</p> <p>NOTE Currently, the built-in alert types cannot be disabled.</p>	<ol style="list-style-type: none"> On the Alarm Type page, select the types to be disabled and click Batch Disable. Alternatively, locate the row containing the alert type to be disabled, click Enable in the Status column. In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the Status of the target type changes to Disable, the target type is disabled successfully.

Parameter	Description
<p>Delete</p> <p>NOTE Currently, built-in alert types cannot be deleted.</p>	<ol style="list-style-type: none"> 1. On the alert type management page, select the type to be deleted and click Delete in the Operation column. 2. In the dialog box displayed, click OK.

----End

11.5.2.2 Managing Incident Types

This section describes how to manage incident types. The detailed operations are as follows:


- **Viewing Incident Types:** describes how to view existing incident types and their details.
- **Adding an Incident Type:** describes how to create custom incident types.
- **Associating an Incident Type with a Layout:** describes how to associate a custom incident type with an existing incident type.
- **Editing an Incident Type:** describes how to edit a custom incident type.
- **Managing Existing Incident Types:** describes how to enable, disable, and delete a custom incident type.

Limitations and Constraints

- By default, built-in incident types are associated with existing layouts. You **cannot** customize associated layouts.
- Built-in incident types are enabled by default and **cannot** be edited, enabled, disabled, or deleted.
- After a customized incident type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

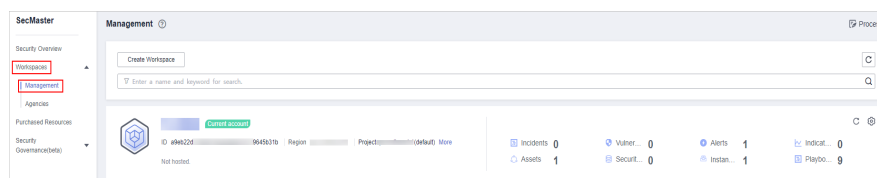
Viewing Incident Types

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

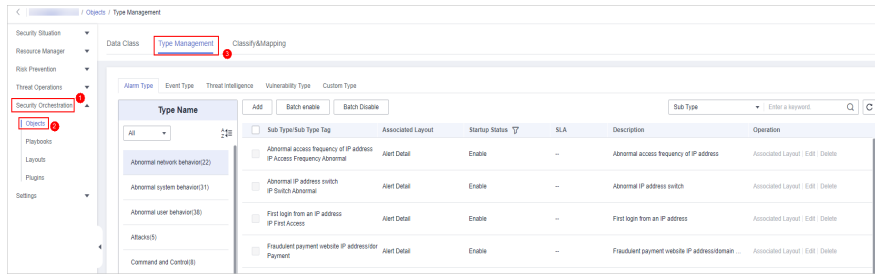
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-23 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-24 Type Management page



Step 5 On the **Types** page, click the **Event Type** tab. The **Event Type** page is displayed.

Step 6 On the **Event Type** page, view the details about existing incident types. For details about the parameters, see [Table 11-9](#).

Figure 11-25 Viewing incident types

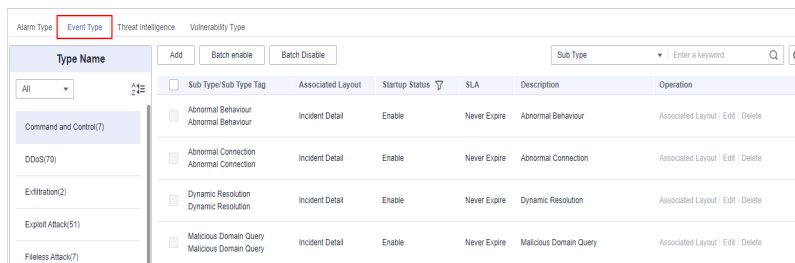



Table 11-9 Incident type parameters

Parameter	Description
Type Name	Name of an incident type
Sub Type/Sub Type Tag	Name and ID of an incident subtype
Associated Layout	Layout associated with the incident type
Startup Status	Indicates whether an incident type is enabled. <ul style="list-style-type: none"> ● Enable: The current type has been enabled. ● Disabled: The current type has been disabled.
SLA	SLA processing time of an incident type
Description	Description of an incident type
Operation	You can edit and delete incident types.

----End

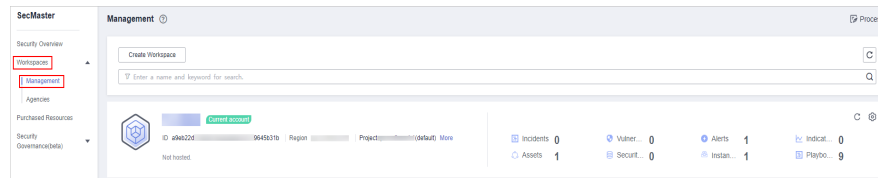
Adding an Incident Type

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

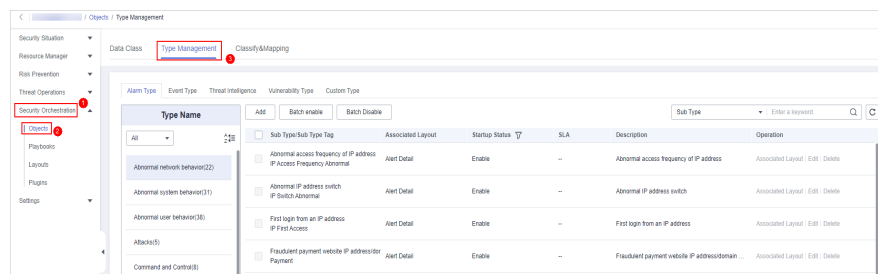
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-26 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-27 Type Management page





Step 5 On the **Types** page, click the **Event Type** tab. The **Event Type** page is displayed.

Step 6 On the **Event Type** page, click **Add**. On the **Add Event Type** slide-out panel, set incident type parameters.

Table 11-10 Incident type parameters

Parameter	Description
Type Name	Customized name of an incident type. The name must comply with the upper camel case naming rules, for example, TypeName .
Type Tag	Enter the incident type ID. The keyword must comply with the upper camel case naming rules, for example, TypeTag .
Sub Type	Enter the subtype of the incident type. The name must comply with the upper camel case naming rules, for example, SubType .
Sub Type Tag	Enter the incident subtype ID. The keyword must comply with the upper camel case naming rules, for example, SubTypeName .

Parameter	Description
Startup Status	Indicates whether an incident type is enabled. <ul style="list-style-type: none">  : indicates that the type is enabled.  : indicates that the alert type is disabled.
SLA	Set the SLA processing time of the incident.
Description	Description of a custom incident type

 **NOTE**

After a customized incident type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

Step 7 In the lower right corner of the page, click **OK**.

After the incident type is added, you can view the new incident type in **Type Name** on the **Event Type** page.


----End

Associating an Incident Type with a Layout

 **NOTE**

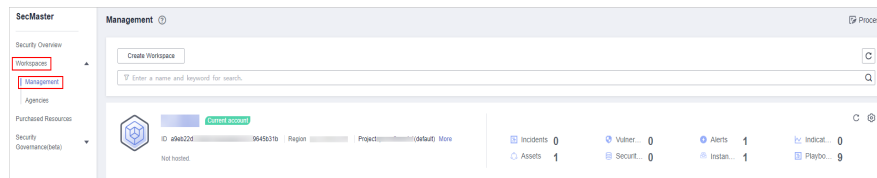
By default, built-in incident types are associated with existing layouts. You cannot customize associated layouts.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

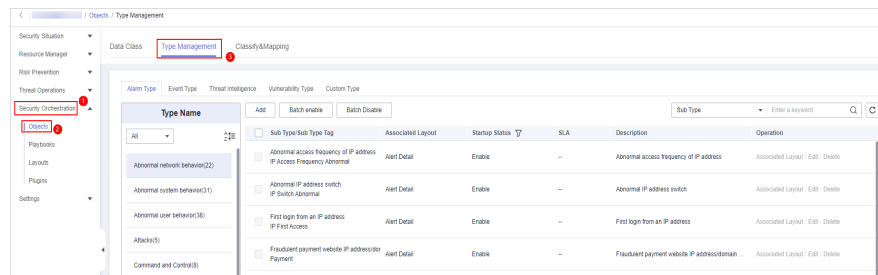
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-28 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-29 Type Management page



Step 5 On the **Types** page, click the **Event Type** tab. The **Event Type** page is displayed.

Step 6 On the **Event Type** page, select the incident type to be associated with a layout and click **Associated Layout** in the **Operation** column of the target type.

Step 7 In the **Associate Layout** dialog box, select the layout to be associated.

Step 8 Click **OK**.


----End

Editing an Incident Type

NOTE

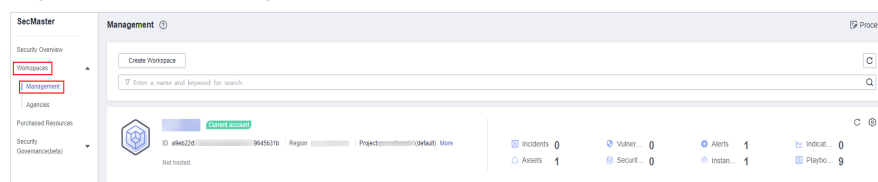
- Currently, the built-in incident type cannot be edited.
- After a customized incident type is added, the **Type Name**, **Type ID**, and **Subtype ID** parameters cannot be modified.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

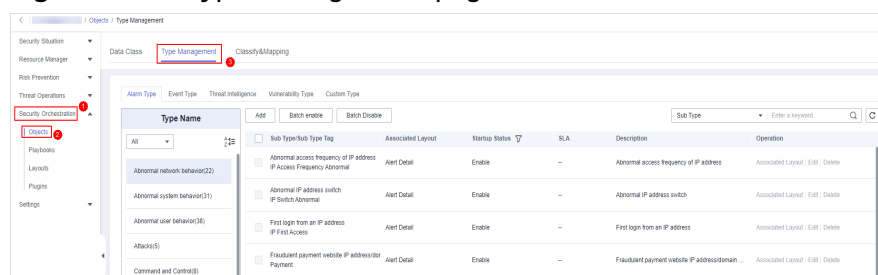
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-30 Management





Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-31 Type Management page



- Step 5** On the **Types** page, click the **Event Type** tab. The **Event Type** page is displayed.
- Step 6** In **Type Name** on the **Alarm Types** page, click the name of the customized incident type to be edited. Details about the custom incident type are displayed on the right.
- Step 7** On the **Event Type** page, click **Edit** in the **Operation** column of the target type to be edited.
- Step 8** In the **Edit Event Type** dialog box, edit parameters.

Table 11-11 Incident type parameters

Parameter	Description
Type Name	Name of an incident type, which cannot be modified.
Type Tag	Incident type ID, which cannot be modified.
Sub Type	Enter the subtype of the incident type.
Sub Type Tag	Incident subtype ID, which cannot be modified.
Startup Status	Indicates whether an incident type is enabled. <ul style="list-style-type: none"> ●  : indicates that the type is enabled. ●  : indicates that the alert type is disabled.
SLA	Set the SLA processing time of the incident.
Description	Description of a custom incident type

- Step 9** In the lower right corner of the page, click **OK**.

----End

Managing Existing Incident Types


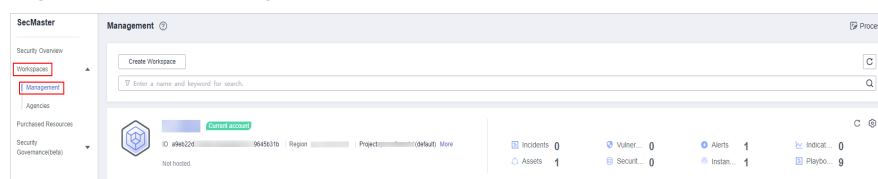
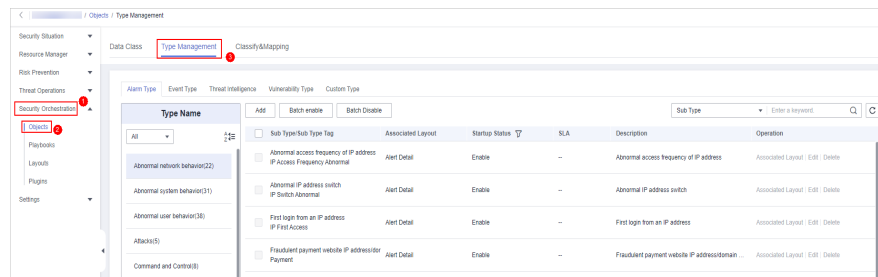
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-32 Management



- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-33 Type Management page



Step 5 On the **Types** page, click the **Event Type** tab. The **Event Type** page is displayed.

Step 6 On the incident type tab, manage incident types.

Table 11-12 Managing existing incident types

Parameter	Description
<p>Enable</p> <p>NOTE The built-in incident types are enabled by default. You do not need to manually enable them.</p>	<ol style="list-style-type: none"> On the type management page, select the type to be enabled and click Batch Enable. Alternatively, locate the row containing the incident type to be enabled, click Disable in the Status column. In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the status of the target type changes to Enable, the target type is enabled successfully.
<p>Disable</p> <p>NOTE Currently, the built-in incident types cannot be disabled.</p>	<ol style="list-style-type: none"> On the Event Type page, select the type to be disabled and click Batch Disable. Alternatively, locate the row containing the incident type to be disabled, click Enable in the Status column. In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the Status of the target type changes to Disable, the target type is disabled successfully.
<p>Delete</p> <p>NOTE Currently, built-in incident types cannot be deleted.</p>	<ol style="list-style-type: none"> On the incident type management page, select the type to be deleted and click Delete in the Operation column. In the dialog box displayed, click OK.

----End

11.5.2.3 Managing Threat Intelligence Types

This section describes how to manage threat intelligence types.

- **Viewing Threat Intelligence Types:** describes how to view existing threat intelligence types and their details.


- **Adding a Threat Intelligence Type:** describes how to create custom threat intelligence types.
- **Associating a Threat Intelligence Type with a Layout:** describes how to associate a custom threat intelligence type with an existing layout.
- **Editing a Threat Intelligence Type:** describes how to edit a custom threat intelligence type.
- **Managing a Threat Intelligence Type:** describes how to enable, disable, and delete a custom threat intelligence type.

Limitations and Constraints

- By default, built-in intelligence types are associated with existing layouts. You **cannot** customize associated layouts.
- Built-in intelligence types are enabled by default and **cannot** be edited, enabled, disabled, or deleted.
- After a user-defined threat intelligence type is added, the type ID **cannot** be modified.

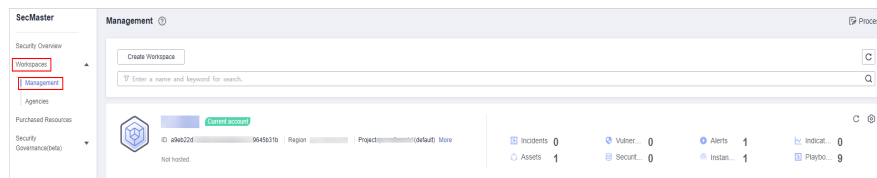
Viewing Threat Intelligence Types

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

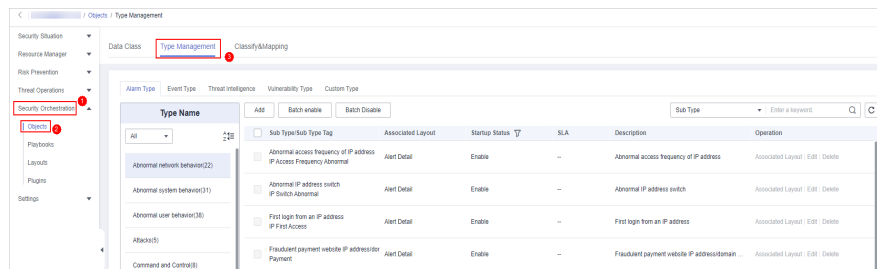
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-34 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-35 Type Management page



Step 5 On the **Type Management** page, click the **Threat Intelligence** tab.

Step 6 On the **Threat Intelligence** page, view details. For details about the parameters, see [Table 11-13](#).

Figure 11-36 Viewing threat intelligence

Type Name/Type Tag	Associated Layout	Startup Status	Expired Time	Built in	Description	Operation
Domain	Domain	Enable	Never Expire	Yes	Domain	Associated Layout Edit Delete
Email	Email	Enable	Never Expire	Yes	Email	Associated Layout Edit Delete
IPv6	IPv6	Enable	Never Expire	Yes	IPv6	Associated Layout Edit Delete
Unclassified	Un_classified	Enable	Never Expire	Yes	Unclassified	Associated Layout Edit Delete
URL	URL	Enable	Never Expire	Yes	URL	Associated Layout Edit Delete
IPv4	IPv4	Enable	Never Expire	Yes	IPv4	Associated Layout Edit Delete

Table 11-13 Threat intelligence type parameters

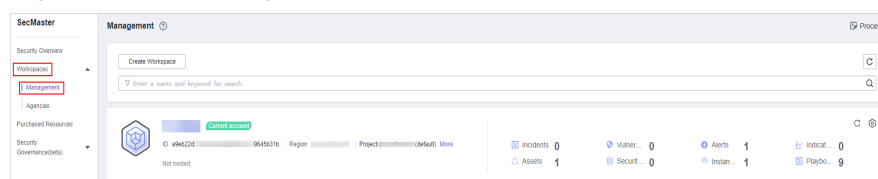
Parameter	Description
Type Name/Type Tag	Name and type tag of threat intelligence
Associated Layout	Layout associated with threat intelligence
Startup Status	Indicates the enabling status of a threat intelligence type: <ul style="list-style-type: none"> ● Enabled: The current type has been enabled. ● Disabled: The current type has been disabled.
Expired Time	Expiration time of threat intelligence.
Built-in	Indicates whether the threat intelligence is built in the system.
Description	Description of a threat intelligence
Operation	You can edit and delete the threat intelligence.

-----End

Adding a Threat Intelligence Type

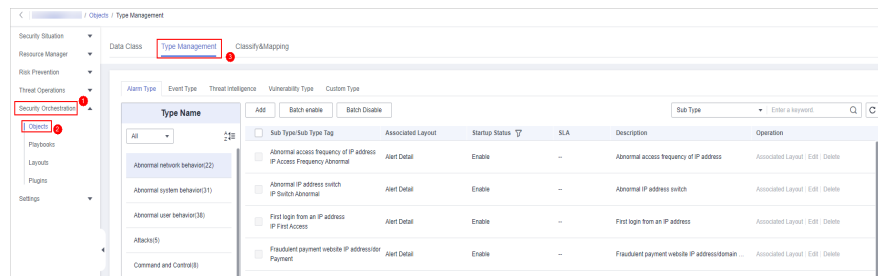
- Step 1** Log in to the management console.
- Step 2** Click in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-37 Management



- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.



Figure 11-38 Type Management page



Step 5 On the **Type Management** page, click the **Threat Intelligence** tab.

Step 6 On the **Threat Intelligence** page, click **Add**. On the **Add Threat Intelligence** slide-out panel, set type parameters.

Table 11-14 Threat intelligence type parameters

Parameter	Description
Type Name	Name of the threat intelligence to be added. The name must comply with the upper camel case naming rules, for example, TypeName .
Type Tag	Enter the threat intelligence type ID. The keyword must comply with the upper camel case naming rules, for example, TypeTag .
Startup Status	Set the enabling status of a threat intelligence. <ul style="list-style-type: none">  : indicates that the type is enabled.  : indicates that the type is disabled.
Expired Time	Set the expiration time of threat intelligence. <ul style="list-style-type: none"> Never Expire: The current intelligence type never expires. Time Interval: Set the interval for invalidating intelligence.
Description	Description of a custom threat intelligence

 **NOTE**

After a user-defined threat intelligence type is added, the type ID **cannot** be modified.

Step 7 In the lower right corner of the page, click **OK**.

After the threat intelligence type is added, you can view the new type in the table on the **Threat Intelligence** page.


----End

Associating a Threat Intelligence Type with a Layout

NOTE

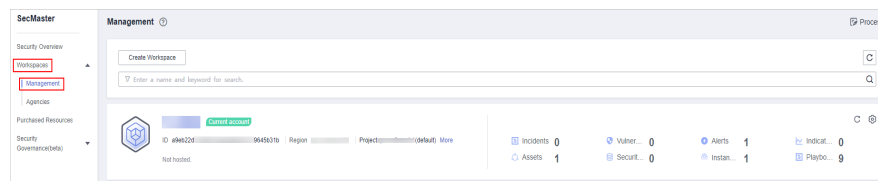
By default, built-in threat intelligence types are associated with existing layouts. You cannot customize associated layouts.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

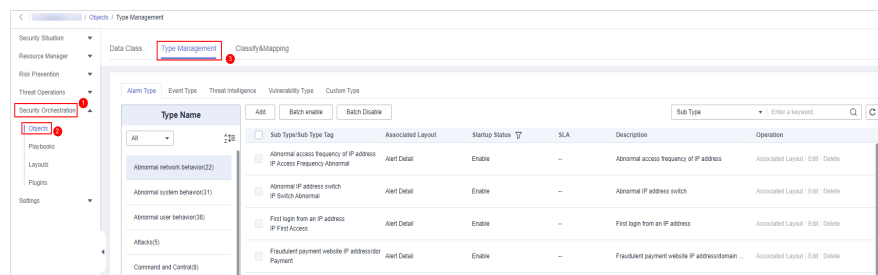
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-39 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-40 Type Management page



Step 5 On the **Type Management** page, click the **Threat Intelligence** tab.

Step 6 On the **Threat Intelligence** page, select the type to be associated with a layout and click **Associated Layout** in the **Operation** column of the target type. The **Associate Layout** dialog box is displayed.

Step 7 In the **Binding/Changing Layouts** box, select the layout to be associated.

Step 8 Click **OK**.


----End

Editing a Threat Intelligence Type

NOTE

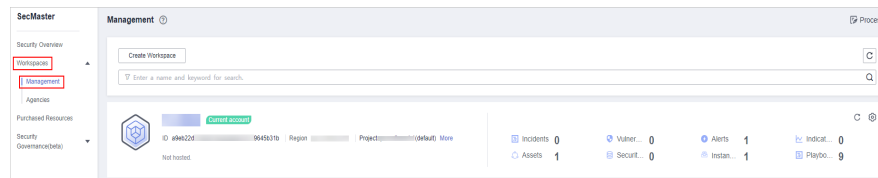
- Currently, built-in threat intelligence types cannot be edited.
- After a user-defined threat intelligence type is added, the type name cannot be modified.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

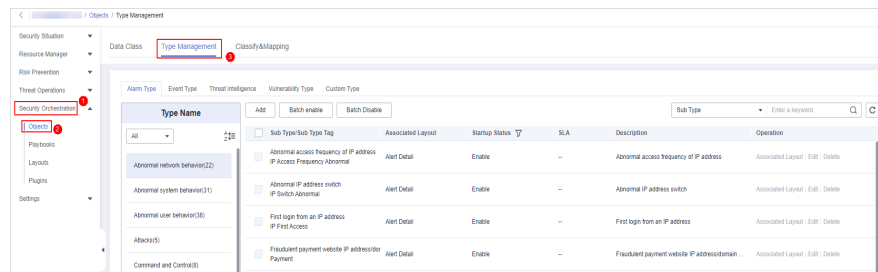
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-41 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-42 Type Management page





Step 5 On the **Type Management** page, click the **Threat Intelligence** tab.

Step 6 On the **Threat Intelligence** page, select the type to be edited and click **Edit** in the **Operation** column of the target type. The editing page is displayed on the right.

Step 7 On the displayed page, edit the parameter information of the corresponding type.

Table 11-15 Threat intelligence type parameters


Parameter	Description
Type Name	Name of the user-defined threat intelligence type.
Type Tag	Threat intelligence type ID, which cannot be modified.
Startup Status	Indicates the enabling status of threat intelligence: <ul style="list-style-type: none">  : indicates that the type is enabled.  : indicates that the type is disabled.
Expired Time	Set the expiration time of threat intelligence. <ul style="list-style-type: none"> Never expire: The current intelligence type never expires. Interval: Set the interval for intelligence type expiration.
Description	Description of a custom threat intelligence type

Step 8 In the lower right corner of the page, click **Confirm**.

----End

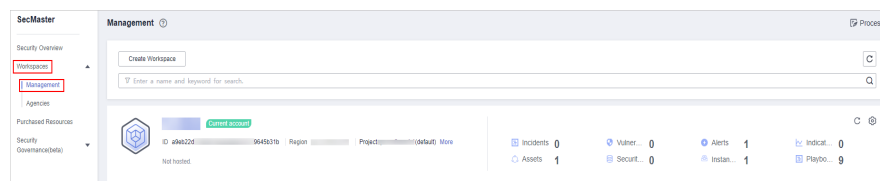
Managing a Threat Intelligence Type

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

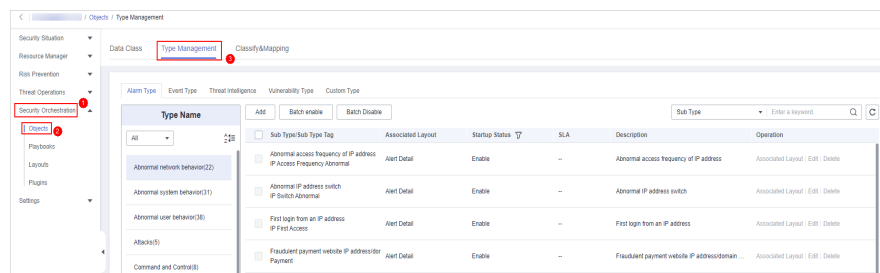
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-43 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-44 Type Management page



Step 5 On the **Type Management** page, click the **Threat Intelligence** tab.

Step 6 On the threat intelligence type tab, manage threat intelligence types.

Table 11-16 Managing a threat intelligence type

Parameter	Description
<p>Enable</p> <p>NOTE Built-in threat intelligence types are enabled by default. You do not need to manually enable them.</p>	<ol style="list-style-type: none"> 1. On the Threat Intelligence page, select the types to be enabled and click Batch enable in the upper left corner of the type list. Alternatively, locate the row containing the threat intelligence to be enabled, click Disable in the Status column. 2. In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the status of the target type changes to Enable, the target type is enabled successfully.
<p>Disable</p> <p>NOTE Currently, built-in threat intelligence types cannot be disabled.</p>	<ol style="list-style-type: none"> 1. On the Threat Intelligence page, select the types to be disabled and click Batch Disable in the upper left corner of the type list. Alternatively, locate the row containing the threat intelligence to be disabled, click Enable in the Status column. 2. In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the Status of the target type changes to Disable, the target type is disabled successfully.
<p>Delete</p> <p>NOTE Currently, built-in threat intelligence types cannot be deleted.</p>	<ol style="list-style-type: none"> 1. On the threat intelligence type management tab, select the type to be deleted and click Delete in the Operation column. 2. In the dialog box displayed, click OK.

----End

11.5.2.4 Managing Vulnerability Types

This section describes how to manage vulnerability types. The detailed operations are as follows:


- **Viewing Existing Vulnerability Types:** Describes how to view existing vulnerability types and their details.
- **Adding a Vulnerability Type:** describes how to create custom vulnerability types.
- **Associating a Vulnerability Type with a Layout:** describes how to associate a custom vulnerability type with an existing layout.
- **Editing a Vulnerability Type:** describes how to edit a custom vulnerability type.
- **Managing a Vulnerability Type:** describes how to enable, disable, and delete a custom vulnerability type.

Limitations and Constraints

- Currently, the built-in vulnerability types of the system do not support customized layouts.
- Built-in vulnerability types are enabled by default and **cannot** be edited, enabled, disabled, or deleted.
- After a user-defined vulnerability type is added, the type ID **cannot** be modified.

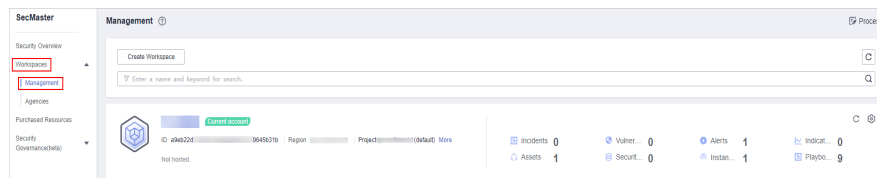
Viewing Existing Vulnerability Types

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

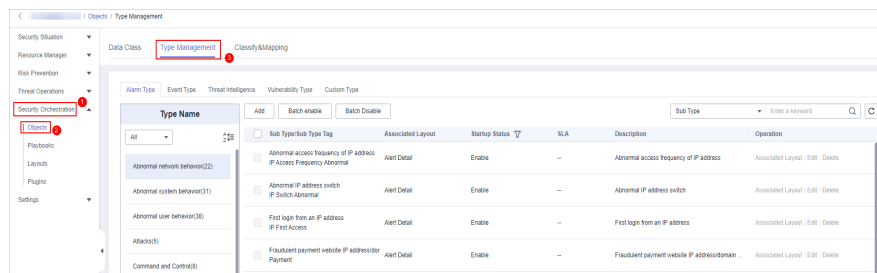
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-45 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-46 Type Management page



Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the **Vulnerability Type** tab page, view details about existing vulnerability types. For details about the parameters, see [Table 11-17](#).

Figure 11-47 Viewing vulnerability types

Type Name	Type Tag	Associated Layout	Startup Status	Built-in	Description	Operation
Linux Vulnerabilities	Linux Vulnerabilities	-	Enable	Yes	Linux Vulnerabilities	Associated Layout Edit Delete
Web-CMS Vulnerabilities	Web-CMS Vulnerabilities	-	Enable	Yes	Web-CMS Vulnerabilities	Associated Layout Edit Delete
Windows Vulnerabilities	Windows Vulnerabilities	-	Enable	Yes	Windows Vulnerabilities	Associated Layout Edit Delete
Application Vulnerabilities	Application Vulnerabilities	-	Enable	Yes	Application Vulnerabilities	Associated Layout Edit Delete


Table 11-17 Vulnerability type parameters

Parameter	Description
Type Name/Type Tag	Name and tag of a vulnerability type
Associated Layout	Layout associated with the vulnerability type.
Startup Status	Indicates the enabling status of a vulnerability type: <ul style="list-style-type: none"> ● Enabled: The current type has been enabled. ● Disabled: The current type has been disabled.
Built-in	Indicates whether the vulnerability is a built-in vulnerability type.
Description	Description of a vulnerability type
Operation	You can edit and delete vulnerability types.

----End

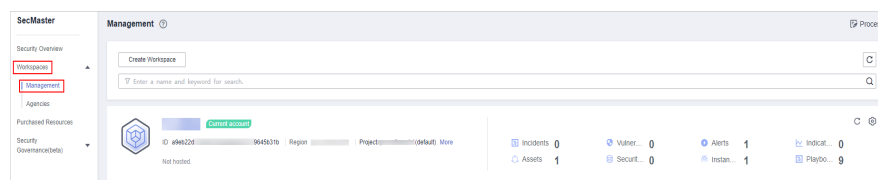
Adding a Vulnerability Type

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

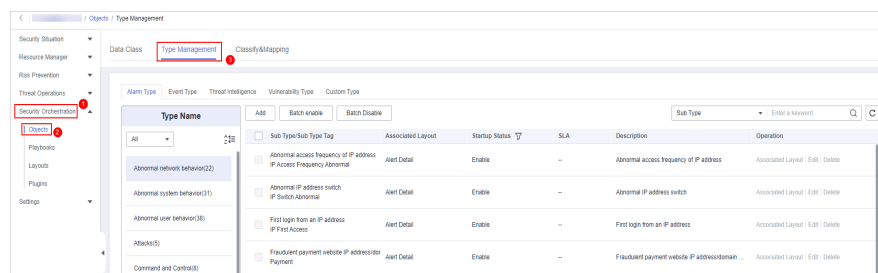
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-48 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.



Figure 11-49 Type Management page



Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the **Vulnerability Type** page, click **Add**. On the **Add Vulnerability Type** slide-out panel, set type parameters.

Table 11-18 Vulnerability type parameters

Parameter	Description
Type Name	Name of the vulnerability type to be added. The name must comply with the upper camel case naming rules, for example, TypeName .
Type Tag	Enter the vulnerability type ID. The keyword must comply with the upper camel case naming rules, for example, TypeTag .
Startup Status	Indicates the enabling status of the vulnerability type: <ul style="list-style-type: none">  : indicates that the type is enabled.  : indicates that the type is disabled.
Description	Description of a user-defined vulnerability

 **NOTE**

After a user-defined vulnerability type is added, the **Type ID** cannot be modified.

Step 7 In the lower right corner of the page, click **Confirm**.

After the threat intelligence type is added, you can view the new type in the table on the **Vulnerability Type** page.


----End

Associating a Vulnerability Type with a Layout

 **NOTE**

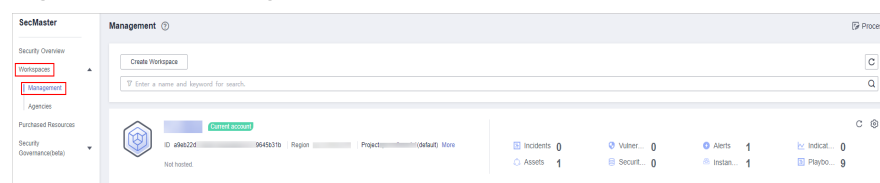
Currently, built-in vulnerability types do not support customized layouts.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

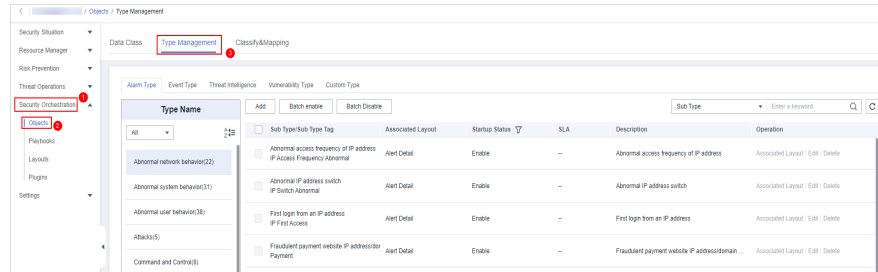
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-50 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-51 Type Management page



Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the **Vulnerability Type** page, select the vulnerability type to be associated with a layout and click **Associated Layout** in the **Operation** column of the target type.

Step 7 In the **Binding/Changing Layouts** box, select the layout to be associated.

Step 8 Click **OK**.


----End

Editing a Vulnerability Type

NOTE

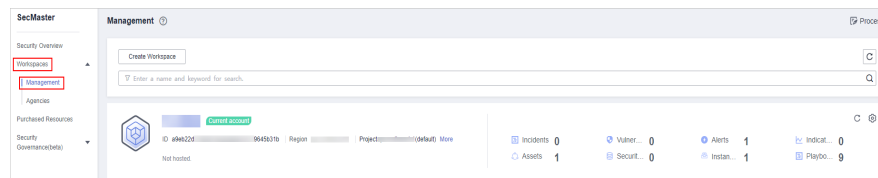
- Currently, the built-in vulnerability types cannot be edited.
- After a user-defined vulnerability type is added, the type ID cannot be modified.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

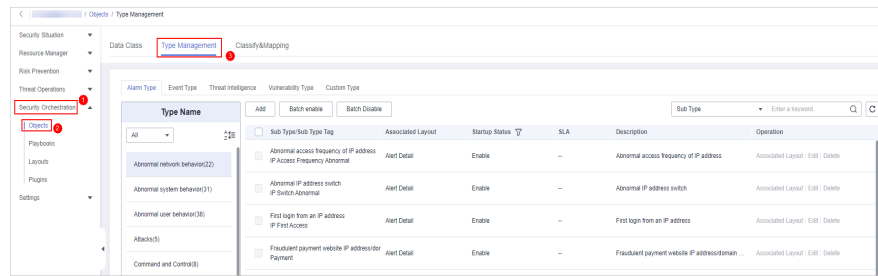
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-52 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-53 Type Management page





Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the **Vulnerability Type** page, select the type to be edited and click **Edit** in the **Operation** column of the target type.

Step 7 On the displayed page, edit the parameter information of the corresponding type.

Table 11-19 Vulnerability type parameters


Parameter	Description
Type Name	Name of a user-defined vulnerability type
Type Tag	Vulnerability type ID, which cannot be modified.
Startup Status	Set the enabling status of the vulnerability type: <ul style="list-style-type: none">  : indicates that the type is enabled.  : indicates that the type is disabled.
Description	Description of a user-defined vulnerability

Step 8 In the lower right corner of the page, click **OK**.

----End

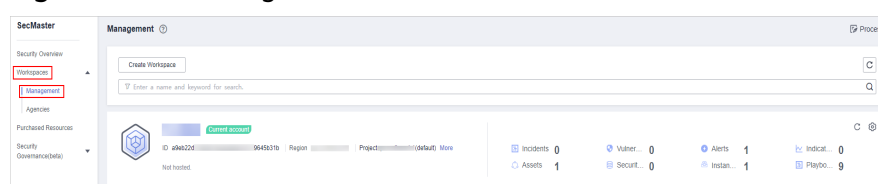
Managing a Vulnerability Type

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

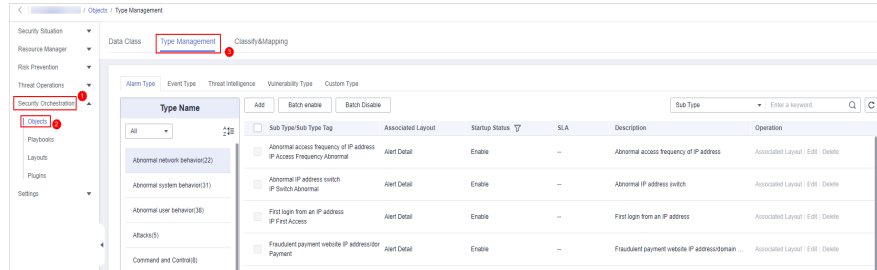
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-54 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Figure 11-55 Type Management page



Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the vulnerability type tab, manage vulnerability types.

Table 11-20 Managing a vulnerability type

Parameter	Description
<p>Enable</p> <p>NOTE Built-in vulnerability types are enabled by default. You do not need to manually enable them.</p>	<ol style="list-style-type: none"> On the Vulnerability Type page, select the type to be enabled and click Batch Enable. Alternatively, locate the row containing the vulnerability type to be enabled, click Disable in the Status column. In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the status of the target type changes to Enable, the target type is enabled successfully.
<p>Disable</p> <p>NOTE Currently, the built-in vulnerability types cannot be disabled.</p>	<ol style="list-style-type: none"> On the Vulnerability Type page, select the type to be disabled and click Batch Disable. Alternatively, locate the row containing the vulnerability type to be disabled, click Enable in the Status column. In the dialog box displayed, click OK. If the system displays a message indicating that the operation is successful and the Status of the target type changes to Disable, the target type is disabled successfully.
<p>Delete</p> <p>NOTE Currently, the built-in vulnerability types cannot be deleted.</p>	<ol style="list-style-type: none"> On the Vulnerability Type tab, select the vulnerability type to be deleted and click Delete in the Operation column. In the dialog box displayed, click OK.

----End

11.5.3 Classification & Mapping

11.5.3.1 Creating a Classification and Mapping

Classification and mapping are to perform class matching and field mapping for cloud service alerts.

This section walks you through on how to create a classification and mapping.

Procedure


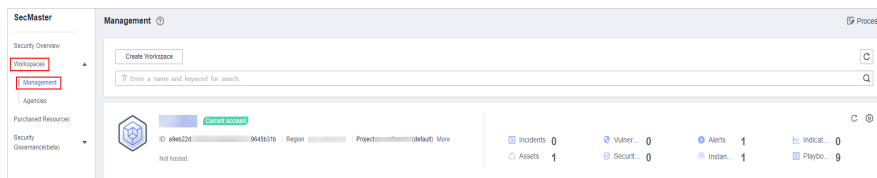
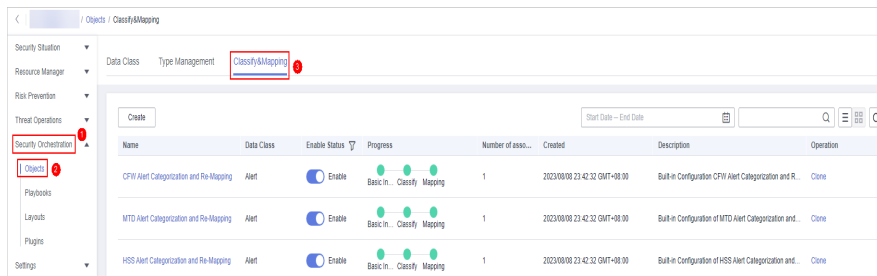
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-56 Management



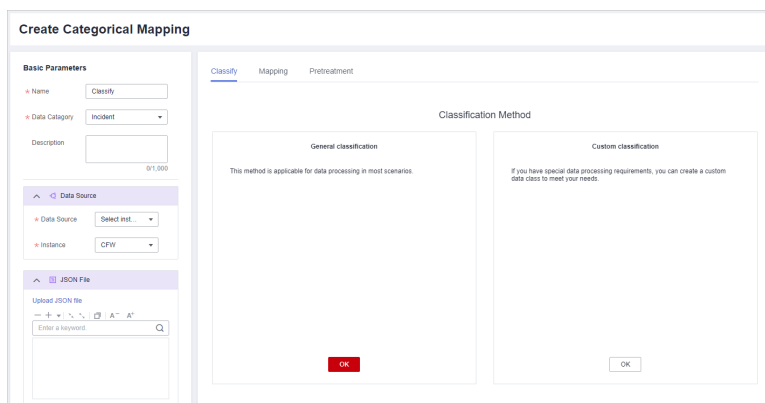
- Step 4** In the navigation pane, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-57 Classify&Mapping tab page



- Step 5** On the **Classify&Mapping** page, click **Create**.
- Step 6** On the **Create Categorical Mapping** page, set category mapping parameters.




Figure 11-58 Create Categorical Mapping page



1. In the **Basic Parameters** area on the left, configure basic information about the category mapping. For details about the parameters, see [Table 11-21](#).

Table 11-21 Configuring basic information

Parameter	Description
Name	Name of a user-defined category mapping.
Data Category	Select the corresponding data type.
Description	Description of the custom categorical mapping.

2. In the **Data Source** area on the left, select the data source for category mapping.
When **Data Source** is set to **Upload JSON file**, you need to click **to upload the JSON file** and upload the JSON file.
3. On the **Classify** tab page on the right, select a classification mode and set related parameters.
4. After the classification configuration is complete, click  at the upper right corner of the page to save the configuration.
5. On the **Mapping** tab page in the right pane, select a mapping mode and set related parameters.
6. After category mapping is complete, click  at the upper right corner of the page to save the configuration.
7. On the **Preprocessing** tab page on the right, set preprocessing mapping parameters.
8. Click  at the upper right corner of the page to save the configuration.

----End

11.5.3.2 Managing Category Mappings

This section describes how to manage category mappings, including [Viewing Category Mappings](#) and [Deleting a Category Mapping](#).

Limitations and Constraints

- Built-in category mappings are enabled by default and **cannot** be edited or deleted.
- When a category mapping is deleted, the plug-ins and connections associated with the category mapping to be deleted are stopped immediately. Deleted category mappings cannot be restored. Exercise caution when performing this operation.
- Non-built-in category mappings cannot be enabled or disabled.

Viewing Category Mappings


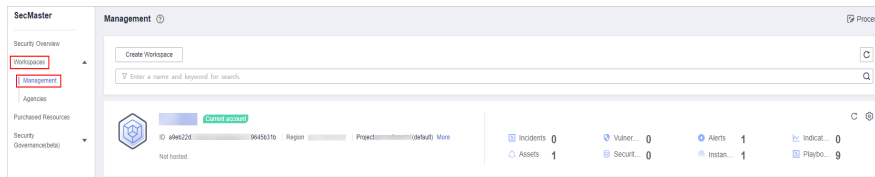
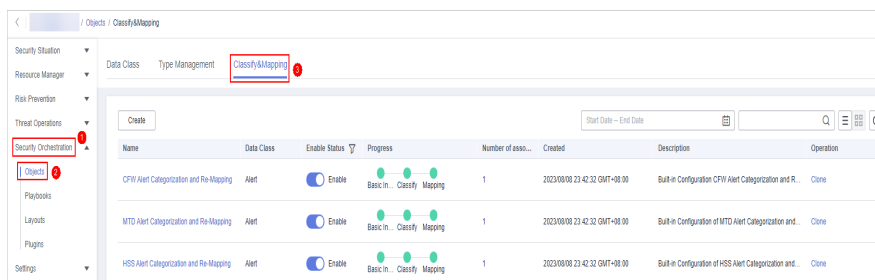
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-59 Management



- Step 4** In the navigation pane, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-60 Classify&Mapping tab page



- Step 5** On the Category Mapping Management page, view details about the created category mapping.

Table 11-22 Category Mapping Information

Parameter	Description
Name	Name of a category mapping.
Data Category	Type of the data class to which the category mapping belongs.
Startup Status	Status of a classification mapping. <ul style="list-style-type: none"> ● Enable: The current category mapping is enabled. ● Disable: The current category mapping has been disabled.
Completion	Completion rate of classification mapping.
Number of associated instances	Total number of plug-in instances associated with category mappings.
Created	Time when a category mapping is created.


Parameter	Description
Description	Description of a categorical mapping.

Step 6 To view details about a category mapping, click the name of the target category mapping. The category mapping details page is displayed.

----End

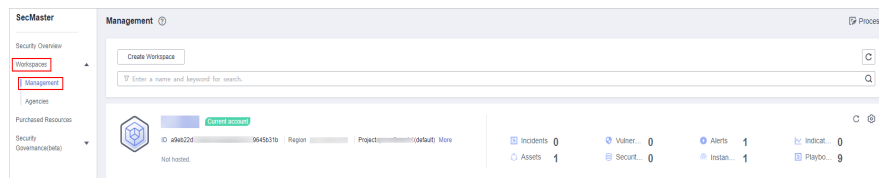
Copying a Category Mapping

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

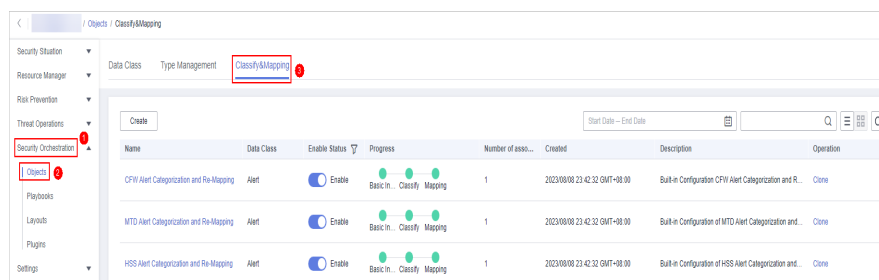
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-61 Management



Step 4 In the navigation pane, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-62 Classify&Mapping tab page



Step 5 On the Category Mapping Management page, click **Copy** in the **Operation** column of the target category mapping.

Step 6 In the displayed dialog box, enter the name of the replication item and click **OK**.


----End

Enabling a Category Mapping

NOTE

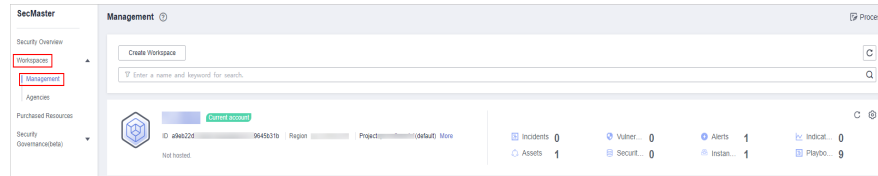
Custom category mappings cannot be enabled.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

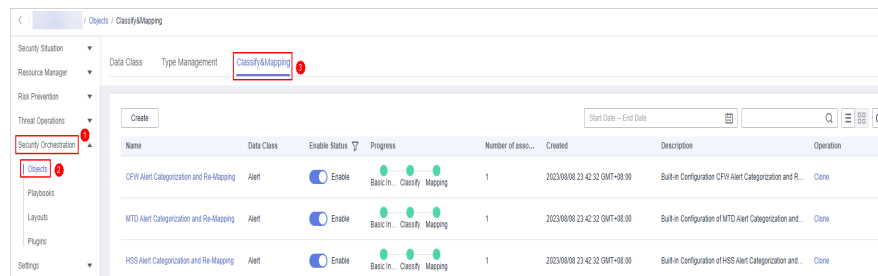
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-63 Management



Step 4 In the navigation pane, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-64 Classify&Mapping tab page



Step 5 On the category mapping management page, locate the row containing your desired category mapping and click **Disable** in the **Status** column.

If the status changes to **Enabled**, the function is successfully enabled.


----End

Disabling a Category Mapping

NOTE

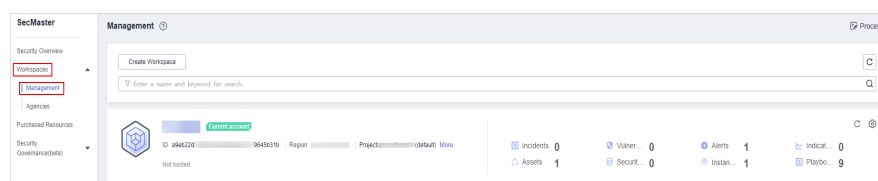
Custom category mappings cannot be disabled.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

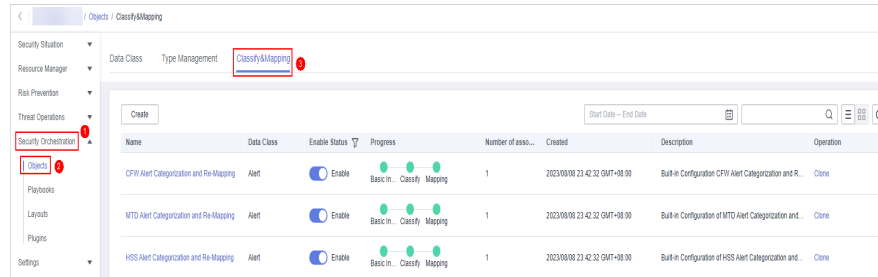
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-65 Management



Step 4 In the navigation pane, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-66 Classify&Mapping tab page



Step 5 On the category mapping management page, locate the row containing your desired category mapping and click **Enable** in the **Status** column.

If the status changes to **Disabled**, the function is successfully disabled.

----End

Deleting a Category Mapping

NOTE

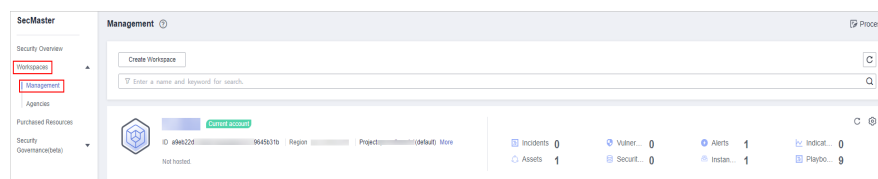
Currently, the built-in category mappings cannot be deleted.

Step 1 Log in to the management console.

Step 2 Click **☰** in the upper left corner of the page and choose **Security > SecMaster**.

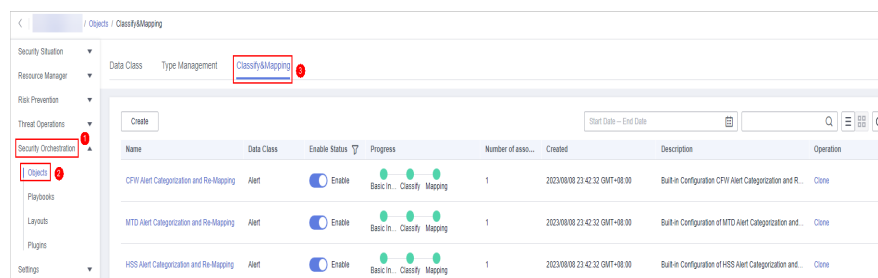
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-67 Management



Step 4 In the navigation pane, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.

Figure 11-68 Classify&Mapping tab page



Step 5 On the Category Mapping Management page, click **Delete** in the **Operation** column of the target category mapping.

Step 6 In the displayed pane on the right, click **Delete**.

NOTE

- When a category mapping is deleted, the plug-ins and connections associated with the category mapping to be deleted are stopped immediately.
- Deleted category mappings cannot be restored. Exercise caution when performing this operation.

----End

11.6 Playbook Orchestration Management

11.6.1 Playbooks

11.6.1.1 Submitting a Playbook Version


This section describes how to submit a playbook version for review.

Prerequisites

The workflow bound to the playbook has been enabled by referring to [Enabling a Workflow](#).

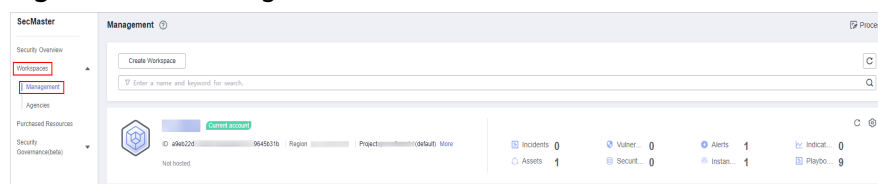
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

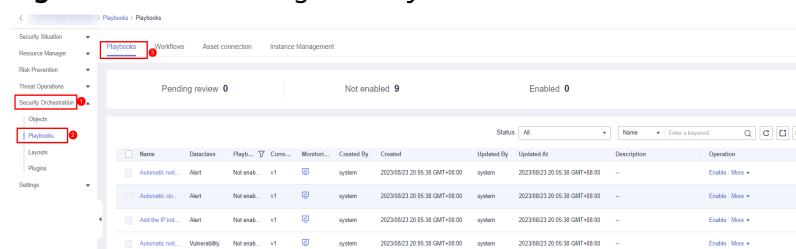
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-69 Management



Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-70 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Submit** in the **Operation** column.

Step 7 In the confirmation dialog box, click **OK** to submit the playbook version.

NOTE

- After the playbook version is submitted, **Version Status** changes to **To be reviewed**.
- After a playbook version is submitted, it cannot be edited. If you need to edit it, you can create a version or reject it during review.

----End

Follow-up Operations

A submitted playbook version needs to be reviewed. For details, see [Reviewing a Playbook Version](#).

11.6.1.2 Reviewing a Playbook Version


This section describes how to review a playbook version.

Prerequisites

The playbook has been submitted by referring to [Submitting a Playbook Version](#).

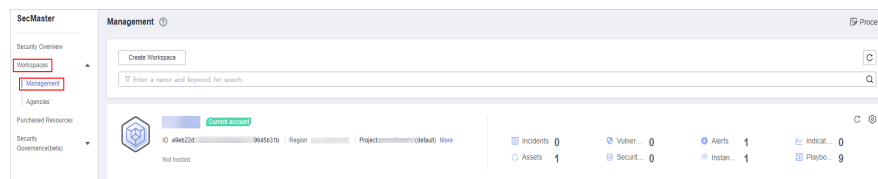
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

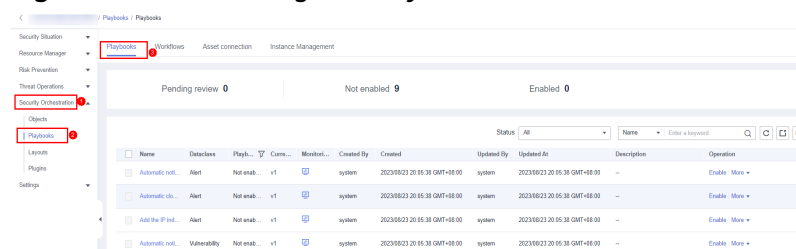
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-71 Management



Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-72 Accessing the Playbooks tab



- Step 5** In the **Operation** column of the target playbook, click **Versions**.
- Step 6** On the **Version Management** slide-out panel, click **Review**.
- Step 7** On the **Review Playbook Version** page, enter the review information. [Table 11-23](#) describes the parameters for reviewing a playbook version.

Table 11-23 Parameters for reviewing a playbook version

Parameter	Description
Comments	<p>Select the review conclusion.</p> <ul style="list-style-type: none"> If the playbook version is approved, the playbook version status changes to Activated. Reject. After the playbook version is rejected, the status of the playbook version changes to Rejected. You can edit the playbook version and submit it again.
Reason for rejection	<p>This parameter is mandatory when the review comment is Reject.</p> <p>Enter the review comment. This parameter is mandatory when Reject is selected for Review Comment.</p>

 **NOTE**

If the current playbook has only one version, the version is in the activated state by default after being approved.

- Step 8** Click **OK** to complete the playbook version review.

----End

Follow-up Operations

An approved playbook version needs to be enabled. For details, see [Enabling a Playbook](#).

11.6.1.3 Enabling a Playbook


After a playbook version is approved, you can enable the playbook. This section describes how to enable a playbook.

Prerequisites

The playbook version has been activated by referring to [Activating/Deactivating a Playbook Version](#).

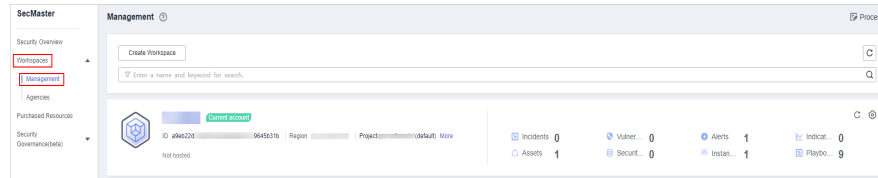
Procedure

- Step 1** Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

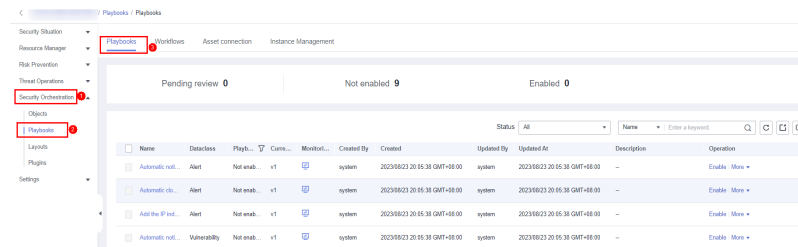
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-73 Management



Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-74 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Enable**.

Step 6 After selecting the playbook version to be enabled, click **OK**.


----End

11.6.1.4 Managing Playbooks

This section describes how to manage playbooks, including [Viewing Existing Playbooks](#), [Importing Playbooks](#), [Exporting Playbooks](#), [Disabling a Playbook](#), and [Deleting a Playbook](#).

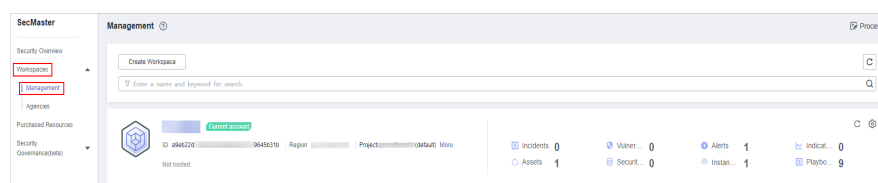
Viewing Existing Playbooks

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

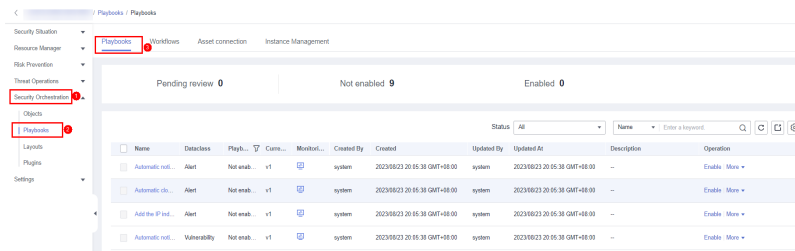
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-75 Management



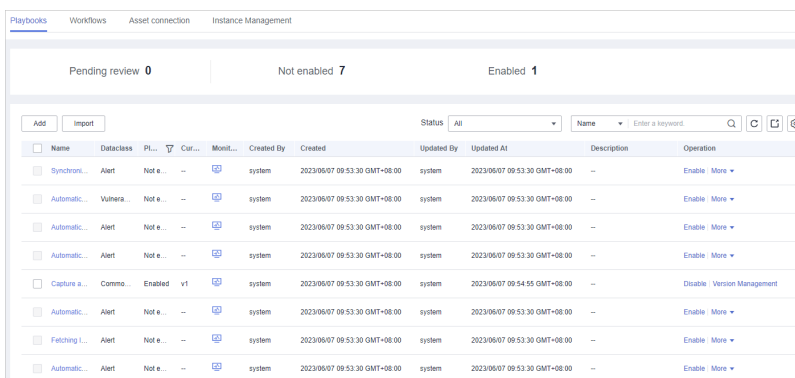
Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-76 Accessing the Playbooks tab



Step 5 On the **Playbooks** tab page, view playbook information.

Figure 11-77 Viewing playbook information



- The numbers of **Pending review**, **Not enabled**, and **Enabled** playbooks are displayed above the playbook list.
- View the information about existing playbooks.



When there are a large number of playbooks, you can use the search function to quickly search for a specified playbook with search filters such as the status, name, description, or data class of the playbook. Enter a keyword in the search box, and click .

Table 11-24 Playbook parameters

Parameter	Description
Name	Name of the playbook to be created.
Dataclass	Data class of the playbook
Playbook Status	Current status of the playbook The status can be Enabled or Disabled.
Current Version	Current version of the playbook


Parameter	Description
Monitoring	<p>Click  to view the playbook running monitoring information.</p> <ul style="list-style-type: none"> - Select Time: Select the monitoring time to be viewed. You can query data in the last 24 hours, last 3 days, last 30 days, or last 90 days. - Edition: Select the monitoring version to be viewed. You can query all, currently valid, and deleted types. - Running Times: You can view the total number of running times, number of scheduled triggering times, and number of incident triggering times of a playbook. - Average Running Duration: allows you to view the average running duration, maximum running duration, and minimum running duration. Average running duration = Total running duration of instances/Total number of instances. - Instance Status Statistics: allows you to view the total number of running instances, the number of successfully running instances, the number of running instances, the number of failed instances, and the number of terminated instances.
Created By	User who creates the playbook
Created	Time when a playbook is created.
Updated By	User who last modified the playbook
Updated At	Time when the playbook was last updated.
Description	Description of a playbook
Operation	You can perform operations such as editing and deleting in the Operation column.

Step 6 To view details about a playbook, click the name of the playbook.

----End

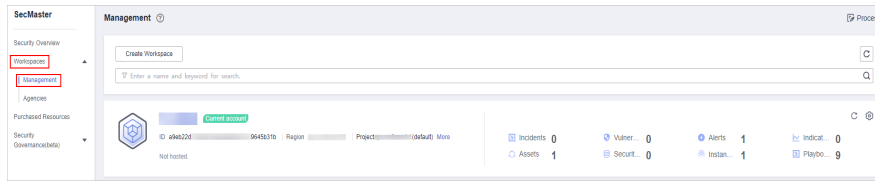
Importing Playbooks

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

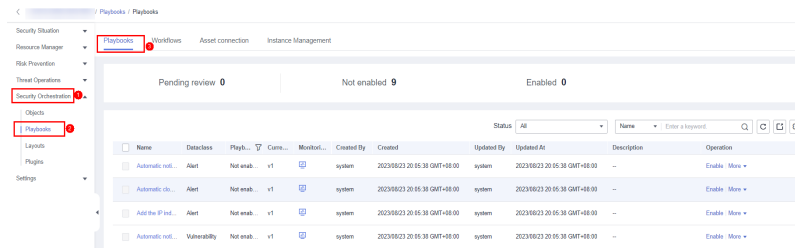
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-78 Management



Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-79 Accessing the Playbooks tab



Step 5 Click **Import** at the upper right corner of the playbook management list. The Import Playbook dialog box is displayed.

Step 6 Click **Select File** and select the file to be imported.

Step 7 Click **Upload**.


----End

Exporting Playbooks

NOTE

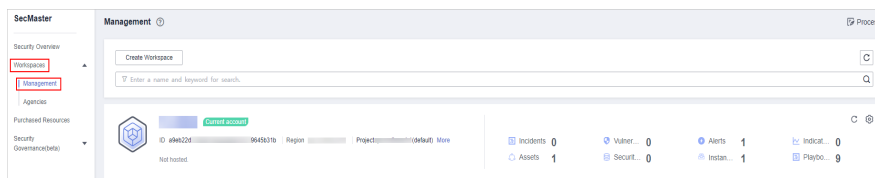
SecMaster supports the export of playbooks whose **Status** is **Enabled**.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

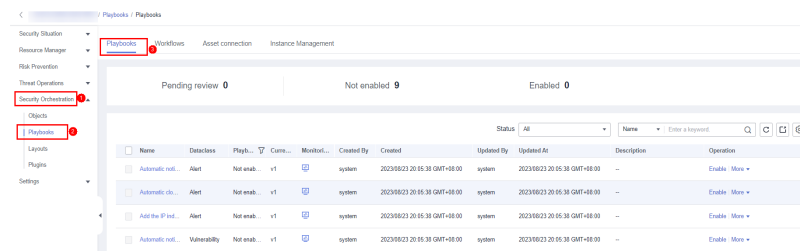
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.


Figure 11-80 Management



Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-81 Accessing the Playbooks tab




Step 5 Select the playbooks to be exported and click  in the upper right corner of the list. The dialog box for confirming the export is displayed.

Step 6 In the dialog box that is displayed, click **OK** to export the playbooks to the local host.

----End

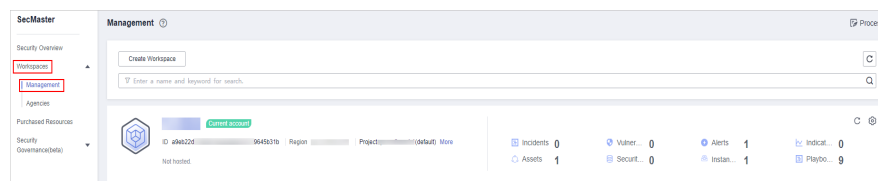
Disabling a Playbook

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

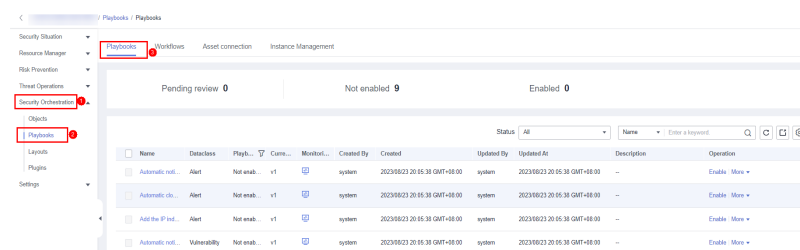
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-82 Management



Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-83 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Disable**. A confirmation dialog box is displayed.

Step 6 In the displayed dialog box, click **OK**.

----End


Deleting a Playbook

NOTE

To delete a playbook, the following conditions must be met:

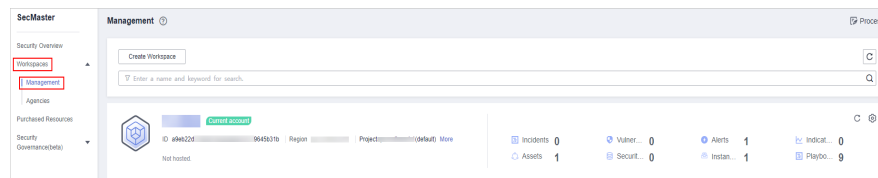
- The playbook is not enabled.
- No activated playbook version exists in the current playbook.
- No running playbook instance exists.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

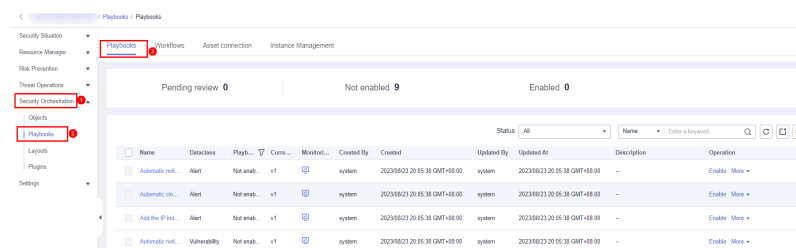
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-84 Management



Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-85 Accessing the Playbooks tab



Step 5 In the **Operation** column of the playbook to be deleted, click **Delete**.

Step 6 In the dialog box that is displayed, click **Confirm** to delete the playbook.

NOTE

By default, all playbook versions in the current playbook are deleted. The deletion operation cannot be undone. Exercise caution when performing this operation.

----End

11.6.1.5 Managing Playbook Versions

This section describes how to manage playbook versions, including [Previewing Playbook Versions](#), [Editing a Playbook Version](#), [Activating/Deactivating a Playbook Version](#), [Copying a Playbook Version](#), and [Deleting a Playbook Version](#).

Previewing Playbook Versions

NOTE

The draft version cannot be previewed.


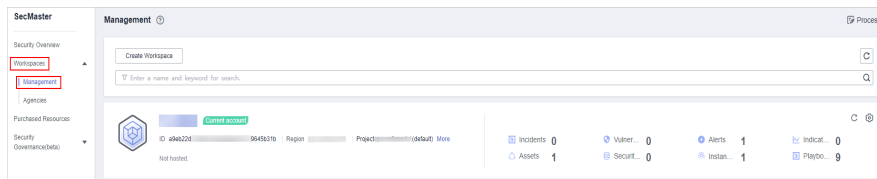
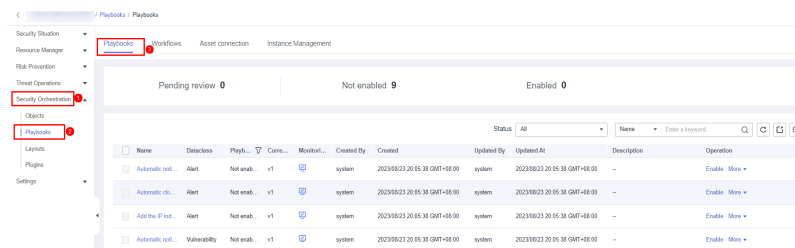
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-86 Management



- Step 4** In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-87 Accessing the Playbooks tab



- Step 5** In the **Operation** column of the target playbook, click **Versions**.
- Step 6** On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Preview** in the **Operation** column.
- Step 7** On the playbook version preview page, you can view the details about the target playbook version, including **Basic Information**, **Version Information**, and **Matching Workflow**.

----End

Editing a Playbook Version

NOTE

Only playbook versions whose version status is **Unsubmitted** can be edited.


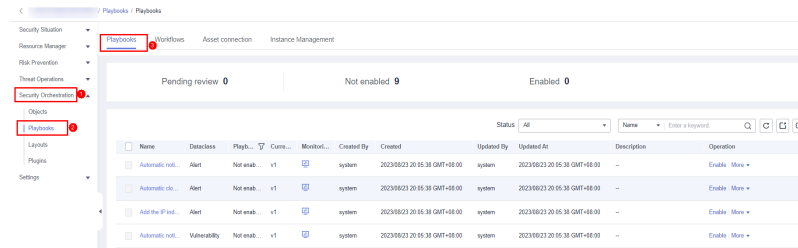
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-88 Accessing the Playbooks tab



Step 4 In the **Operation** column of the target playbook, click **Versions**.

Step 5 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Edit** in the **Operation** column.

Step 6 On the page for editing a playbook version, edit the version information.

Step 7 Click **OK**.


----End

Activating/Deactivating a Playbook Version

NOTE

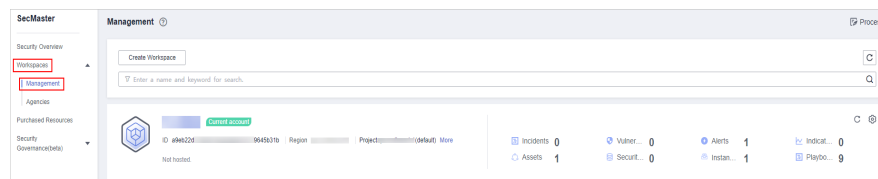
- Only the playbook version that is not activated can be activated.
- Only one activated version is allowed for each playbook.
- After the current version is activated, the previously activated version is deactivated. For example, if the V2 version is activated this time, the V1 version in the activated state is deactivated and changes to the deactivated state.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

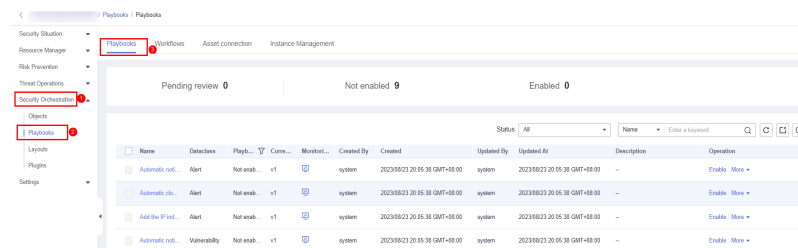
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-89 Management



Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-90 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Step 6 On the **Version Management** page, in the version information area, locate the row containing the desired playbook version, and click **Activate** or **Deactivate** in the **Operation** column.


----End

Copying a Playbook Version

NOTE

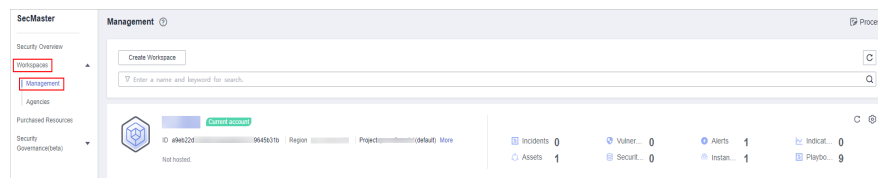
Only playbook versions in the **Activated** or **Inactive** state can be copied.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

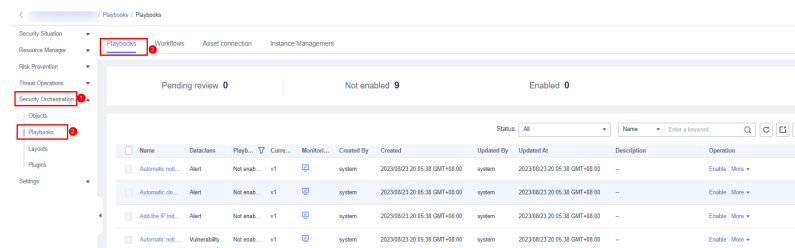
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-91 Management



Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-92 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Copy** in the **Operation** column.

Step 7 In the dialog box that is displayed, click **OK**.

----End


Deleting a Playbook Version

NOTE

To delete a playbook version, the following conditions must be met:

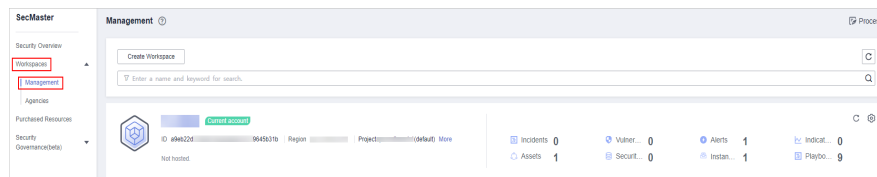
- The playbook version is inactivated.
- No running playbook version instance exists.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

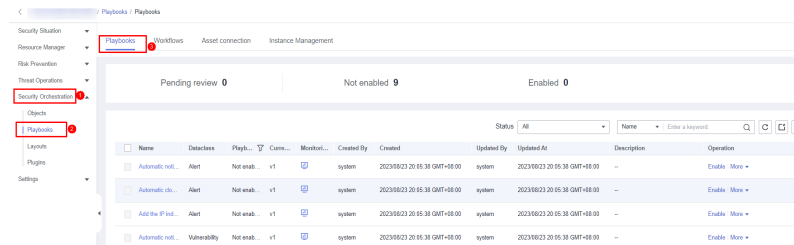
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-93 Management



Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**.

Figure 11-94 Accessing the Playbooks tab



Step 5 In the **Operation** column of the target playbook, click **Versions**.

Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired playbook version, and click **Delete** in the **Operation** column.

NOTE

After a playbook version is deleted, it cannot be retrieved. Exercise caution when performing this operation.

----End

11.6.2 Workflows

11.6.2.1 Reviewing a Workflow Version

This topic describes how to review a workflow version.

Procedure


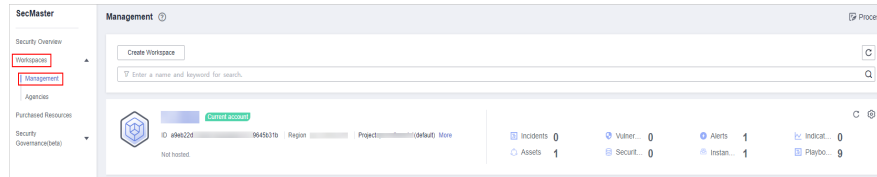
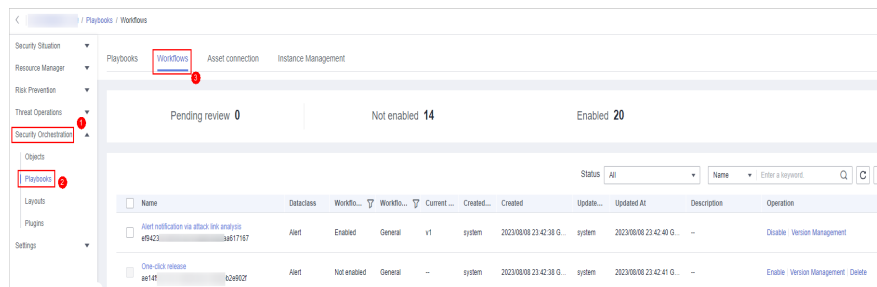
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-95 Management



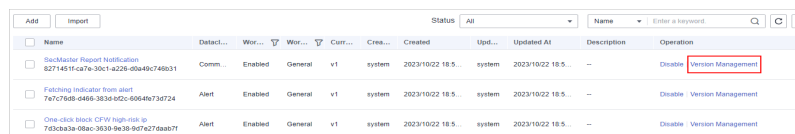
- Step 4** In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-96 Workflows tab page



- Step 5** In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-97 Version Management page



- Step 6** On the **Version Management** slide-out panel, click **Review** in the **Operation** column of the target workflow.
- Step 7** Set **Comments**. [Table 11-25](#) describes the parameters.

Table 11-25 Workflow review parameters

Parameter	Description
Comments	<p>Select the review conclusion.</p> <ul style="list-style-type: none"> If the workflow version is approved, the status of the workflow version changes to Activated. Reject. After the workflow version is rejected, the status of the workflow version changes to Rejected. You can edit the workflow version and submit it again.
Reason for rejection	Enter the review comment. This parameter is mandatory when Reject is selected for Review Comment.

NOTE

- You can edit a rejected workflow version. For details, see [Managing Workflow Versions](#).
- Workflow version status change:
If the current workflow has only one workflow version, the status of the approved workflow **version** is **Activated** by default.

Step 8 Click **OK** to complete the workflow version review.

----End

Follow-up Operations

An approved workflow version needs to be enabled. For details, see [Enabling a Workflow](#).

11.6.2.2 Enabling a Workflow

This section describes how to enable a workflow.

Prerequisites

A workflow version has been activated by referring to [Managing Workflow Versions](#).

Procedure


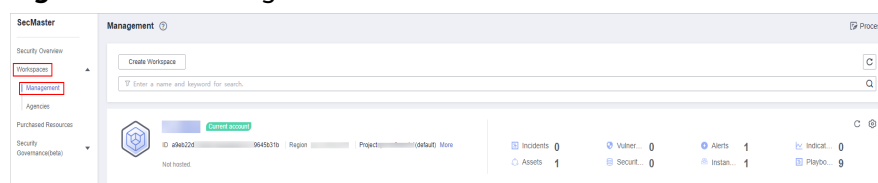
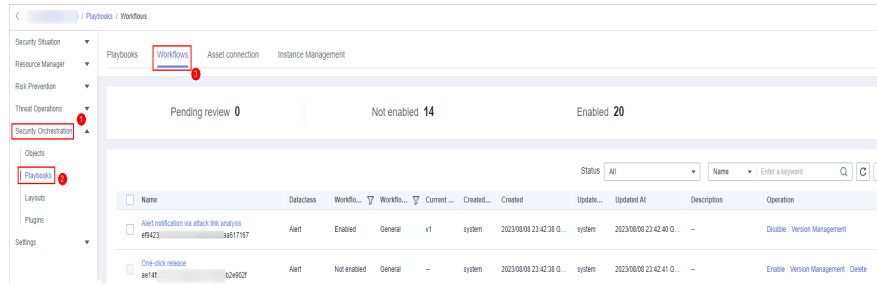
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-98 Management



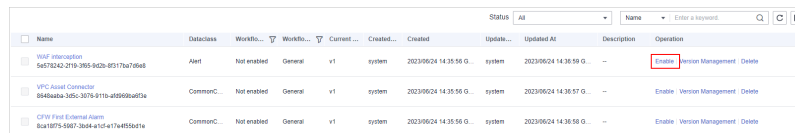
Step 4 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-99 Workflows tab page



Step 5 In the row containing the target workflow, click **Enable** in the **Operation** column.

Figure 11-100 Enabling a workflow



Step 6 In the slide-out panel that is displayed, select the workflow version to be enabled and click **OK**.

----End

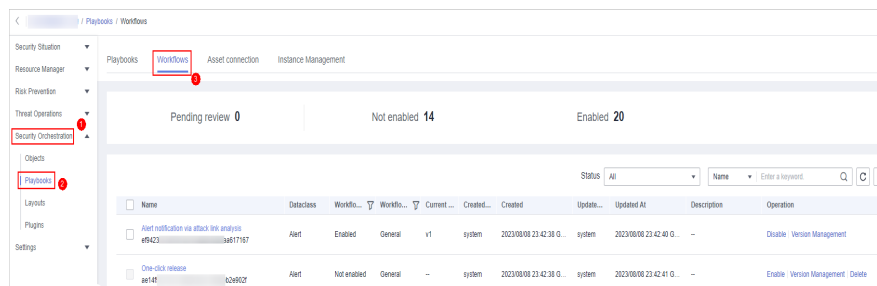
11.6.2.3 Managing Workflows

This section describes how to manage workflows, including **Viewing Workflows**, **Importing Workflows**, **Exporting Workflows**, **Deleting Workflows**, and **Disabling a Workflow**.

Viewing Workflows

Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-101 Workflows tab page



Step 2 On the Workflow Management page, view the information about the created workflow.

Figure 11-102 Viewing workflows

- The numbers of **Pending review**, **Not enabled**, and **Enabled** workflows are displayed above the workflow list.
- View information about existing workflows in the workflow list.
If there are a large number of workflows, you can select the workflow status, name, description, or data class, enter a keyword in the search box, and click to quickly search for a specified workflow.

Table 11-26 Workflow parameters

Parameter	Description
Name	Workflow name
Dataclass	Data class corresponding to a workflow.
Workflow Status	Current status of a workflow. The status can be Enabled or Disabled .
Workflow Type	Current type of a workflow.
Current Version	Current version of a workflow.
Created By	User who creates the workflow.
Created	Time when a workflow was created
Updated By	User who modifies the workflow last time.
Updated At	Time when a workflow is last updated.
Description	A description of the workflow.
Operation	You can perform operations such as enabling and managing versions in the Operation column.

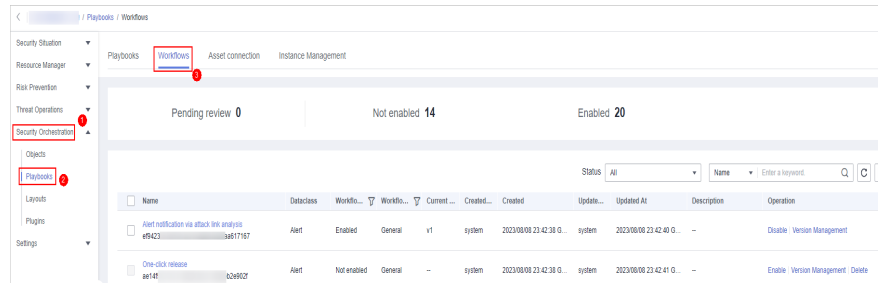
Step 3 To view details about a workflow, click the name of the workflow to access its details page.

----End

Importing Workflows

Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-103 Workflows tab page



Step 2 In the upper right corner of the workflow management list, click **Import**.

Step 3 Click **Select File** and select the file to be imported.

Step 4 Click **Upload**.

----End

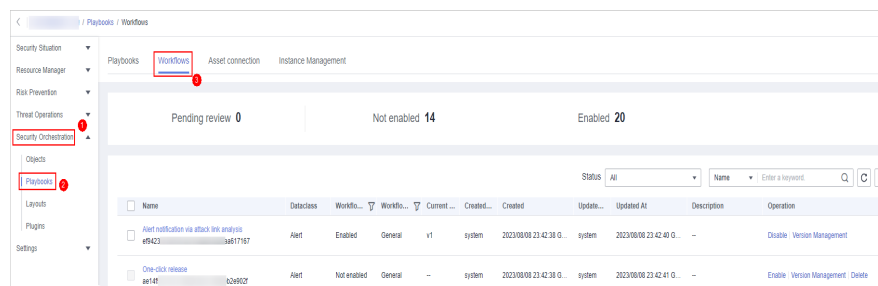
Exporting Workflows


NOTE

Workflows in the **Enabled** state can be exported.

Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-104 Workflows tab page



Step 2 On the **Workflows** tab page, select the workflows to be exported and click  in the upper right corner of the list.

Step 3 In the dialog box that is displayed, click **OK**. The system exports the workflows to the local host.

----End

Deleting Workflows

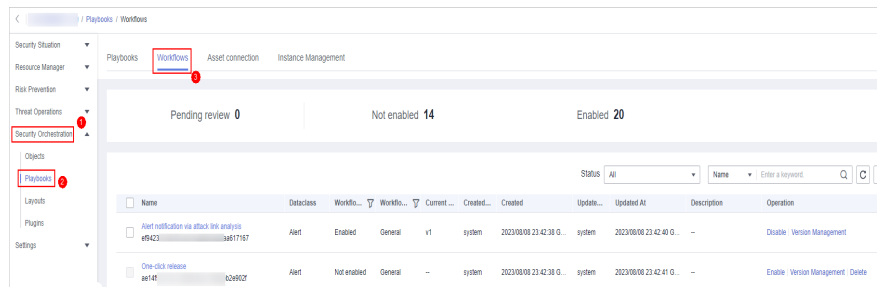
NOTE

All of the following conditions must be met before you can delete a workflow:

- The workflow is in the **Disabled** state.
- The workflow does not contain an activated workflow version.

Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-105 Workflows tab page



Step 2 On the **Workflows** tab page, locate the row containing the target workflow and click **Delete** in the **Operation** column.

Step 3 Click **OK** to delete the workflow.

NOTE

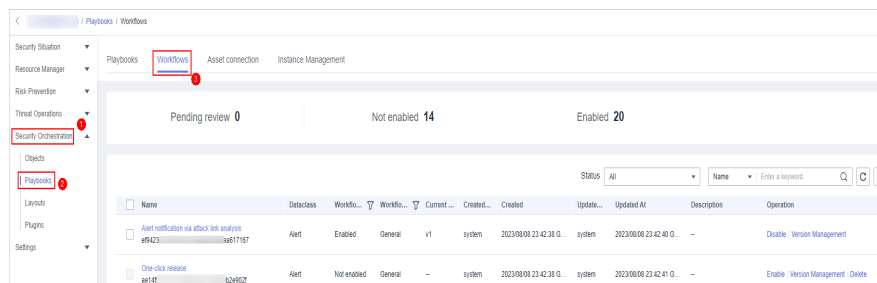
During deletion, all historical versions in the current workflow are deleted by default. Deleted versions cannot be restored.

----End

Disabling a Workflow

Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-106 Workflows tab page



Step 2 In the row containing the target workflow, click **Disable** in the **Operation** column.

Step 3 In the dialog box that is displayed, click **OK**.

----End

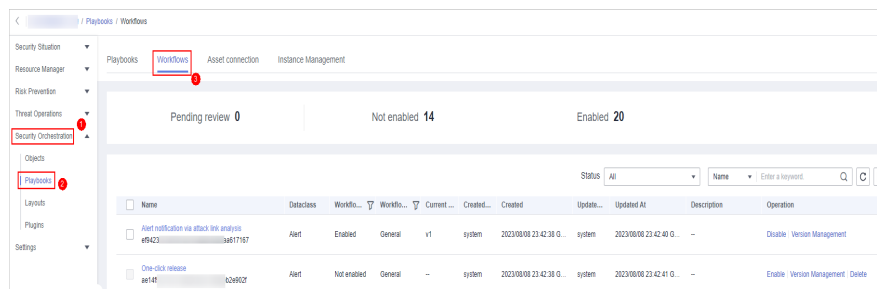
11.6.2.4 Managing Workflow Versions

This section describes how to manage workflow versions, including [Copying a Workflow Version](#), [Editing a Workflow Version](#), [Submitting a Workflow Version](#), [Activating/Deactivating a Workflow Version](#), and [Deleting a Workflow Version](#).

Copying a Workflow Version

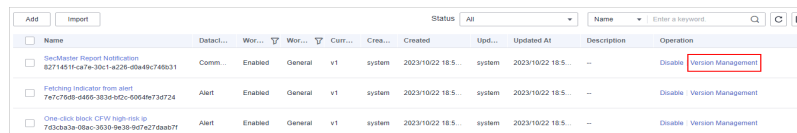
Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-107 Workflows tab page



Step 2 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-108 Version Management page



Step 3 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Copy** in the **Operation** column.

Step 4 In the dialog box displayed, click **OK**.

----End

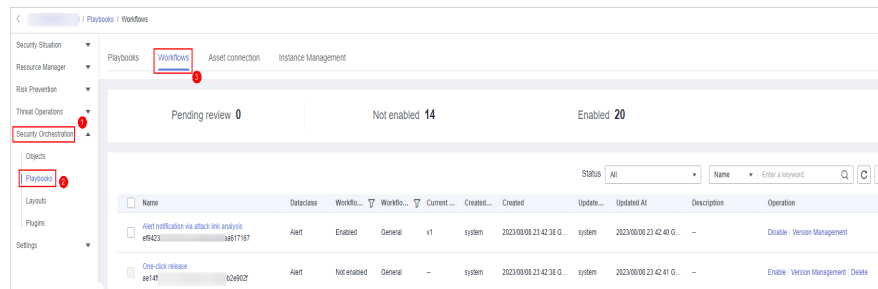
Editing a Workflow Version

NOTE

You can only edit a workflow version whose version status is **To be submitted** or **Rejected**.

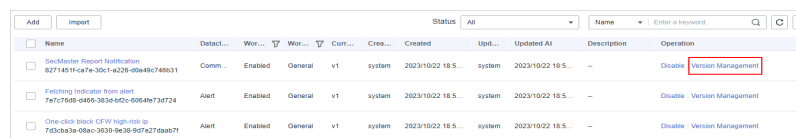
Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-109 Workflows tab page



Step 2 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-110 Version Management page



Step 3 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Edit** in the **Operation** column.

Step 4 On the workflow drawing page, drag basic, workflow, and plug-in nodes from **Resource Libraries** on the left to the canvas on the right for workflow design.

Table 11-27 Resource Libraries parameters

Parameter		Description	
Basic	Basic Node	StartEvent	The start of a workflow. Each workflow can have only one start node. The entire workflow starts from the start node.
		EndEvent	The end of a workflow. Each workflow can have multiple end nodes, but the workflow must end with an end node.
		UserTask	When the workflow execution reaches this node, the workflow is suspended and a to-do task is generated on the Task Center page. After you complete the task, the subsequent nodes in the workflow continue to be executed. Table 11-28 describes the UserTask parameters.
		SubProcess	Another workflow is started to perform cyclic operations. It is equivalent to the loop body in the workflow.

Parameter			Description
	System Gateway	ExclusiveGateway	During line distribution, one of the multiple lines is selected for execution based on the condition expression. During line aggregation, if one of the multiple lines arrives, the subsequent nodes continue to execute the task.
		ParallelGateway	During line distribution, all lines are executed. During line aggregation, the subsequent nodes are executed only when all the lines arrive. (If one line fails, the entire workflow fails.)
		InclusiveGateway	During line distribution, all expressions that meet the conditions are selected for execution based on the condition expression. During line aggregation, subsequent nodes are executed only when all lines executed during traffic distribution reach the inclusive gateway. (If one line fails, the entire workflow fails.)
Workflows			You can select all released workflows in the current workspace.
Plug-ins			You can select all plug-ins in the current workspace.

Table 11-28 UserTask parameters

Parameter	Description
Primary key ID	The system automatically generates a primary key ID, which can be changed as required.
Workspace Name	Name of the manual review node
Expired	Expiration time of a manual review node
Description	Description of the manual review node
View Parameters	Click >> . On the Select Context page that is displayed, select an existing parameter name. To add a parameter, click Add Parameter .
Manual Handling Parameters	Key of the input parameter To add a parameter, click Add Parameter .

Parameter	Description
Processed By	<p>Set the reviewer of the workflow to the IAM user of the current account. If a workflow needs to be approved after the setting, only the owner can handle it on the Task Center page. Non-owners can only view the workflow.</p> <p>NOTE In first time use, you need to obtain authorization. Detailed operations are as follows:</p> <ol style="list-style-type: none"> 1. Click Authorize. 2. On the Access Authorization slide-out panel displayed, select Agree and click OK.

Step 5 After the design is complete, click **Save and Submit** in the upper right corner. In the automatic workflow verification dialog box displayed, click **OK**.

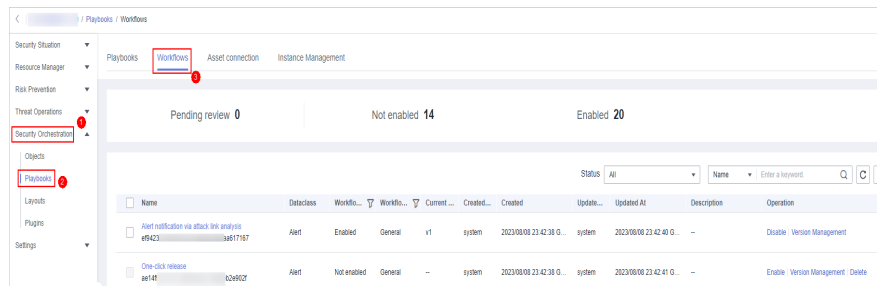
If the workflow verification fails, check the workflow based on the failure message.

----End

Submitting a Workflow Version

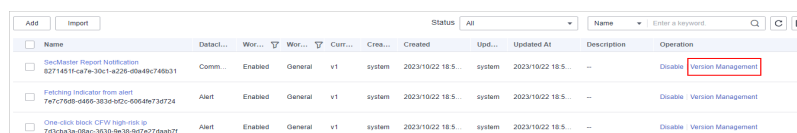
Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-111 Workflows tab page



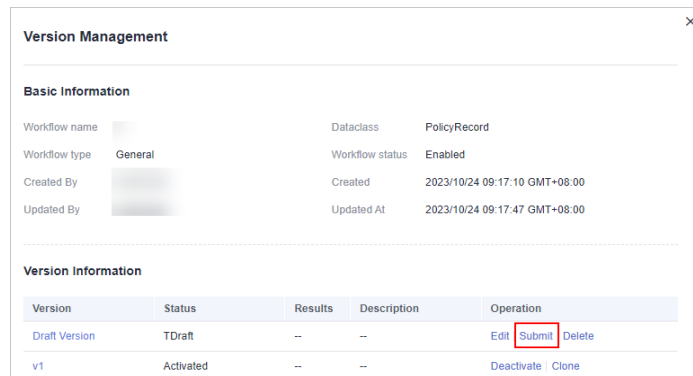
Step 2 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-112 Version Management page



Step 3 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Submit** in the **Operation** column.

Figure 11-113 Submitting a workflow version



Step 4 In the confirmation dialog box, click **OK** to submit the workflow version.

NOTE

- After the workflow version is submitted, the **Version Status** changes to **Pending Review**.
- After a workflow version is submitted, it cannot be edited. If you need to edit it, you can create a version or reject it during review.

----End

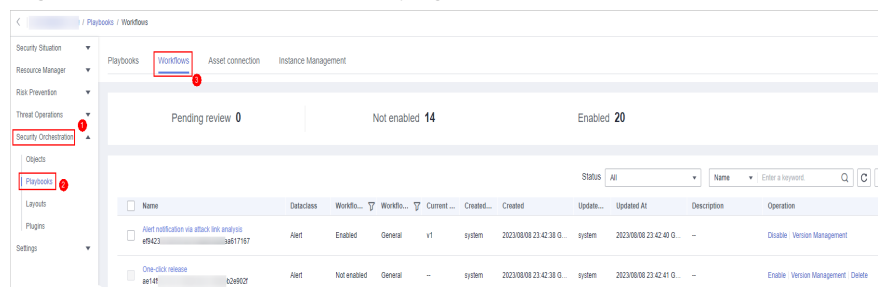
Activating/Deactivating a Workflow Version

NOTE

- Only workflow versions in the **Inactive** state can be activated.
- Each workflow can have only one activated version.
- After the current version is activated, the previously activated version is deactivated. For example, if the V2 version is activated this time, the V1 version in the activated state is deactivated and changes to the deactivated state.

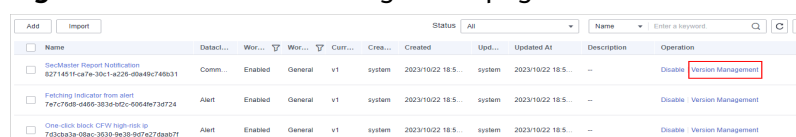
Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-114 Workflows tab page



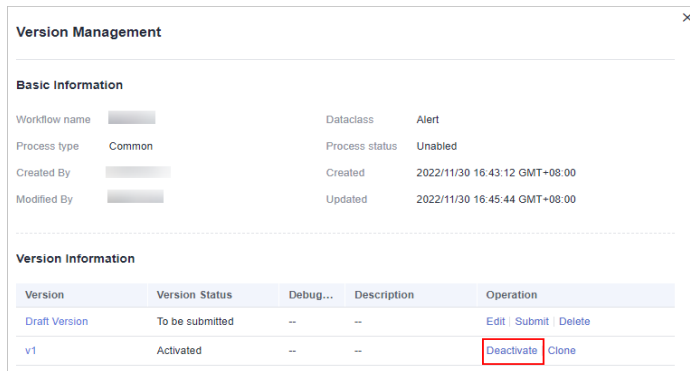
Step 2 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-115 Version Management page



Step 3 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Activate** or **Deactivate** in the **Operation** column.

Figure 11-116 Example deactivating a workflow version



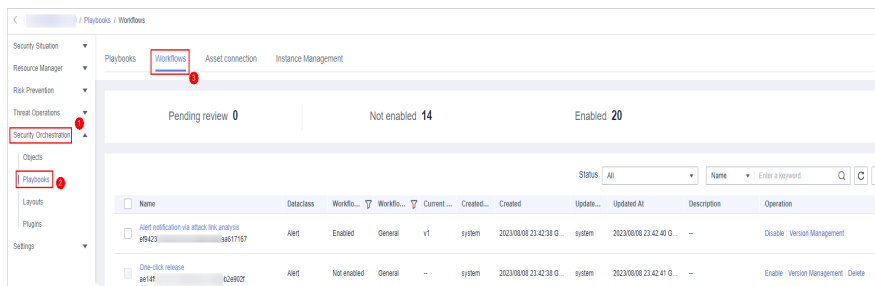
Step 4 In the dialog box that is displayed, click **OK**.

----End

Deleting a Workflow Version

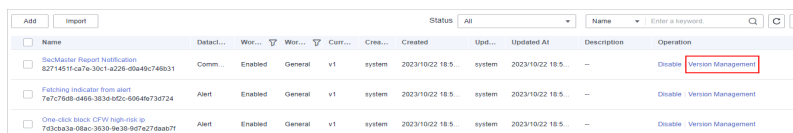
Step 1 In the left navigation pane, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Figure 11-117 Workflows tab page



Step 2 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Figure 11-118 Version Management page



Step 3 On the **Version Management** slide-out panel, in the version information area, locate the row containing the desired workflow version, and click **Delete** in the **Operation** column. In the dialog box displayed, click **OK**.

 NOTE

Deleted workflow versions cannot be retrieved. Exercise caution when performing this operation.

----End

11.6.3 Asset Connections

11.6.3.1 Adding an Asset Connection

This topic describes how to create an asset.

Prerequisites

A workspace has been created by referring to [Creating a Workspace](#).

Procedure


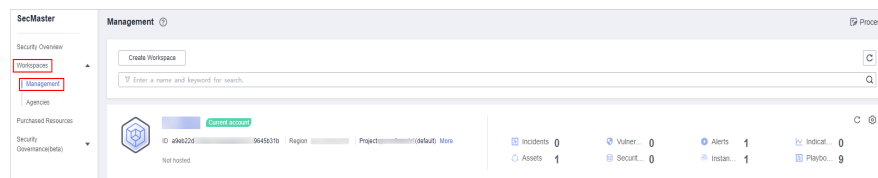
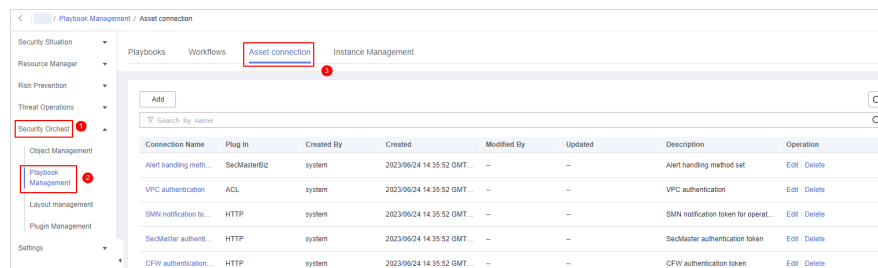
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-119 Management



- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-120 Asset connection tab page



- Step 5** On the **Asset Connection** tab page, click **Add**. The slide-out panel **Add** is displayed on the right.
- Step 6** On the panel, set asset connection parameters. For details about the parameters, see [Table 11-29](#).

Table 11-29 Asset connection parameters

Parameter	Description
Connection Name	Enter an asset connection name. The naming rules are as follows: <ul style="list-style-type: none"> Only uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and underscores (_) are allowed. A maximum of 64 characters are allowed.
Description	(Optional) Enter the asset description. The description can contain a maximum of 64 characters.
Plug In	Select the plug-in required for asset connection. For details about the plug-in, see Viewing Plug-in Details .

Step 7 Click **OK**. You can query the created asset connection in the asset connection list.


----End

11.6.3.2 Managing Asset Connections

This topic describes [Viewing Asset Connections](#), [Editing an Asset Connection](#), and [Deleting an Asset Connection](#).

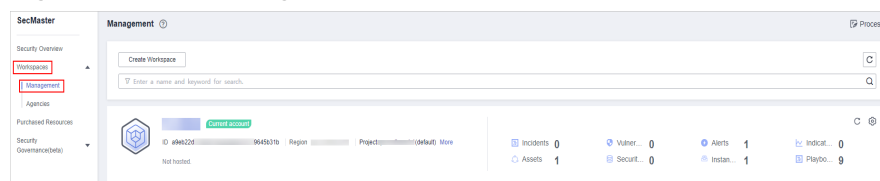
Viewing Asset Connections

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

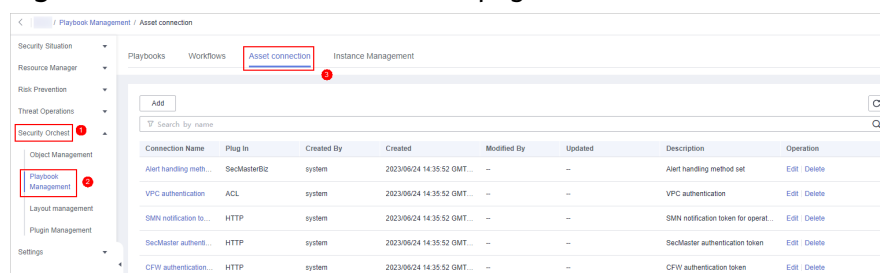
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-121 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-122 Asset connection tab page



Step 5 On the **Asset connection** tab page, view information about existing asset connections.


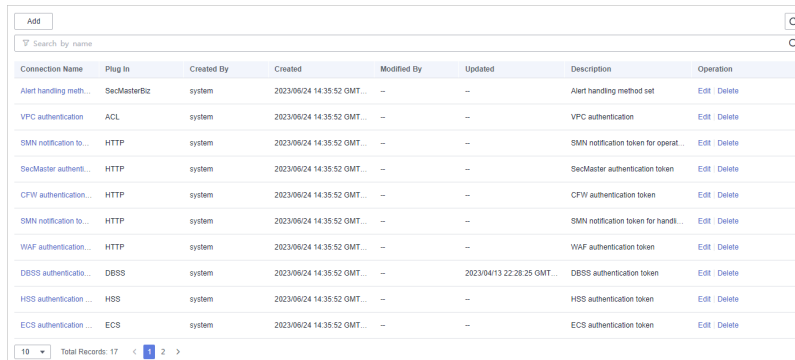
If there are a large number of asset connections, you can use the search function to quickly search for a specified asset connection: Filter asset connections by connection name, plug-in, creator, creation time, person who modified the connection, update time, or description of an asset connection, enter a keyword in the search box, and click .

Figure 11-123 Viewing asset connections



Connection Name	Plug In	Created By	Created	Modified By	Updated	Description	Operation
Alert handling meth.	SecMasterBiz	system	2023/09/24 14:35:52 GMT...	--	--	Alert handling method set	Edit Delete
VPC authentication	ACL	system	2023/09/24 14:35:52 GMT...	--	--	VPC authentication	Edit Delete
SMN notification to.	HTTP	system	2023/09/24 14:35:52 GMT...	--	--	SMN notification token for operat...	Edit Delete
SecMaster authent.	HTTP	system	2023/09/24 14:35:52 GMT...	--	--	SecMaster authentication token	Edit Delete
CFW authentication...	HTTP	system	2023/09/24 14:35:52 GMT...	--	--	CFW authentication token	Edit Delete
SMN notification to.	HTTP	system	2023/09/24 14:35:52 GMT...	--	--	SMN notification token for handl...	Edit Delete
WAF authentication...	HTTP	system	2023/09/24 14:35:52 GMT...	--	--	WAF authentication token	Edit Delete
DBSS authentication...	DBSS	system	2023/09/24 14:35:52 GMT...	--	2023/04/13 22:28:25 GMT...	DBSS authentication token	Edit Delete
HSS authentication ...	HSS	system	2023/09/24 14:35:52 GMT...	--	--	HSS authentication token	Edit Delete
ECS authentication ...	ECS	system	2023/09/24 14:35:52 GMT...	--	--	ECS authentication token	Edit Delete

Table 11-30 Asset connection parameters


Parameter	Description
Connection Name	Asset connection name
Plug In	Plug-in corresponding to the asset connection
Created By	User who creates an asset connection
Created	Time when an asset connection is created
User who last updated the information	User who modifies the asset connection last time
Updated	Time when the asset connection was last updated
Description	Description of the asset connection
Operation	You can perform operations such as editing and deleting in the Operation column.

Step 6 To view details about an asset connection, click the name of the asset connection. The slide-out panel **Detail** is displayed.

----End

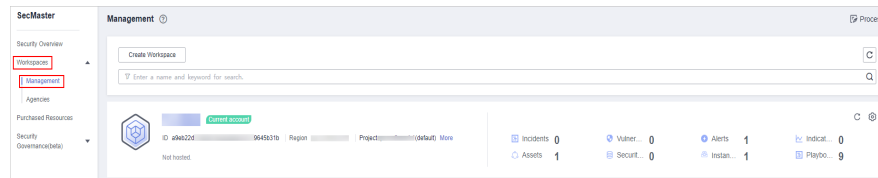
Editing an Asset Connection

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

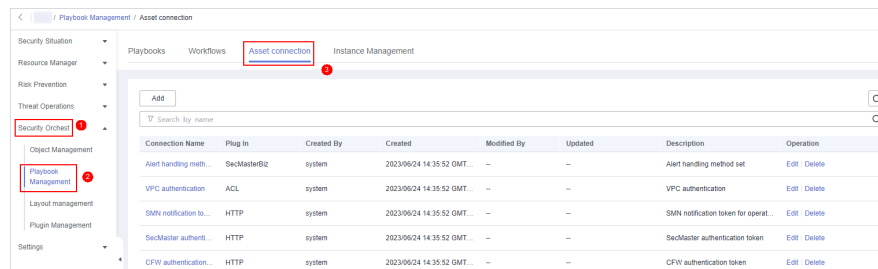
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-124 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-125 Asset connection tab page



Step 5 In the row containing a desired asset connection, click **Edit** in the **Operation** column. The slide-out panel **Edit** is displayed.

Step 6 On the **Edit** panel, edit asset connection parameters. For details about the parameters, see [Table 11-31](#).

Table 11-31 Asset connection parameters

Parameter	Description
Connection Name	Enter an asset connection name. The naming rules are as follows: <ul style="list-style-type: none"> Only uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and underscores (_) are allowed. A maximum of 64 characters are allowed.
Description	(Optional) Enter the asset connection description. The description can contain a maximum of 64 characters.
Plug In	Select the plug-in required for asset connection. For details about the plug-in, see Viewing Plug-in Details .
Created By	Creator of the asset connection. This parameter cannot be modified .


Parameter	Description
Created	Time when an asset connection is created. This parameter cannot be modified .
Modified By	User who last modifies the asset connection. This parameter cannot be modified .

Step 7 Click **OK**.

----End

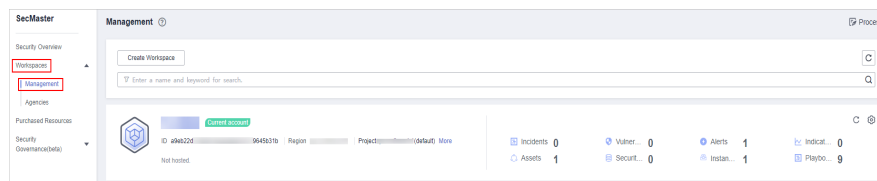
Deleting an Asset Connection

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

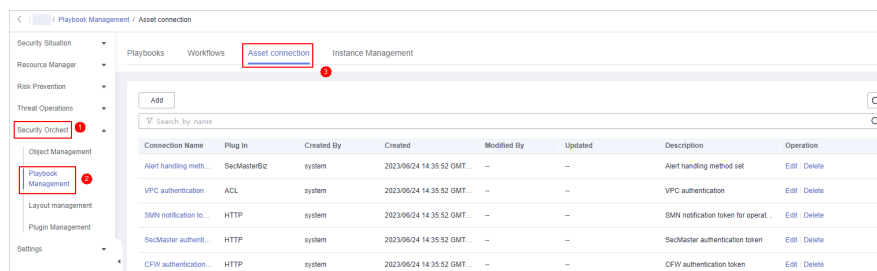
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-126 Management



Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**. On the displayed page, click the **Asset Connections** tab.

Figure 11-127 Asset connection tab page



Step 5 Locate the row that contains a desired asset connection, click **Delete** in the **Operation** column.

Step 6 In the deletion confirmation dialog box that is displayed, click **OK** to confirm the deletion.

 **NOTE**

Deleted assets cannot be restored. Exercise caution when performing this operation.

----End

11.6.4 Instance Management

11.6.4.1 Viewing Monitored Playbook Instances

After a playbook is executed, a playbook instance is generated in the playbook instance management list for monitoring. Each record in the instance monitoring list is an instance. You can view the historical instance task list and the statuses of historical instance tasks.

View instance monitoring information.

Limitations and Constraints

The maximum number of manual retries of a workflow instance is 3. A workflow instance can be retried only after the playbook execution is complete.

Procedure


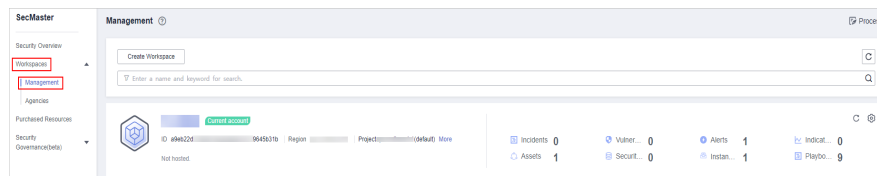
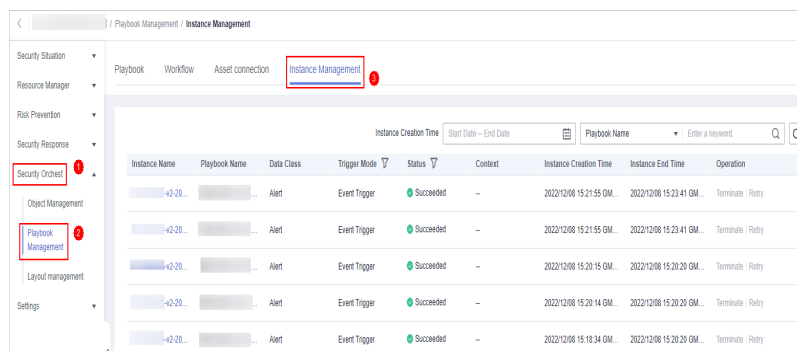
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-128 Management



- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. On the displayed page, click the **Instance Management** tab.

Figure 11-129 Instance Management page



- Step 5** In the instance management list, view the instance name, playbook name, and data class. For details about the parameters, see [Table 11-32](#).

Figure 11-130 Instances

Instance Name	Playbook Name	Data Class	Trigger Mode	Status	Context	Instance Creation Time	Instance End Time	Operation
CSZMGJCFv1-20...		Alert	Event Trigger	Running	--	2022/11/30 16:48:35 GM...	--	Terminate Retry
GJCF1-v3-202211...		Alert	Event Trigger	Running	--	2022/11/30 15:28:40 GM...	--	Terminate Retry
GJCF1-v3-202211...		Alert	Event Trigger	Running	--	2022/11/30 15:28:30 GM...	--	Terminate Retry
GJCF1-v3-202211...		Alert	Event Trigger	Succeeded	--	2022/11/30 15:28:30 GM...	2022/11/30 15:33:32 G...	Terminate Retry
GJCF1-v3-202211...		Alert	Event Trigger	Running	--	2022/11/30 15:28:30 GM...	--	Terminate Retry
GJCF1-v3-202211...		Alert	Event Trigger	Running	--	2022/11/30 15:28:30 GM...	--	Terminate Retry
GJCF1-v2-202211...		Alert	Event Trigger	Succeeded	--	2022/11/30 15:16:52 GM...	2022/11/30 15:16:54 G...	Terminate Retry
GJCF1-v2-202211...		Alert	Event Trigger	Succeeded	--	2022/11/30 15:16:50 GM...	2022/11/30 15:28:34 G...	Terminate Retry
GJCF1-v2-202211...		Alert	Event Trigger	Succeeded	--	2022/11/30 15:16:49 GM...	2022/11/30 15:28:33 G...	Terminate Retry

Table 11-32 Parameters in the instance list

Parameter	Description
Instance Name	Name of an instance
Playbook Name	Name of the playbook corresponding to the instance.
Data Class	Operation object of a playbook
Trigger Mode	Triggering mode of an instance <ul style="list-style-type: none"> ● Timer Trigger ● Incident Trigger
Status	Status of an instance <ul style="list-style-type: none"> ● Succeeded: The playbook instance is successfully executed. ● Failed: The playbook instance fails to be executed. You can click Retry in the Operation column to execute the playbook again. ● Running: The playbook instance is running. You can click Terminate in the Operation column to terminate the playbook. ● Retrying: The playbook instance is being retried. ● Terminating: The playbook instance is being terminated. ● Stopped: The playbook instance has been terminated.
Context	Context information of an instance
Instance Creation Time	Time when an instance is created.
Instance End Time	Time when an instance ends.
Operation	You can perform operations such as termination and retry.

Step 6 To view details about an instance, click the instance name. On the displayed page, you can view the instance workflow and workflow node information.

----End

11.7 Layout Management

11.7.1 Viewing an Existing Layout Template

The management page and details page templates for alert management, incident management, vulnerability management, analysis report, intelligence management, and large-screen security are available in the layout.

View an existing layout template.

Procedure


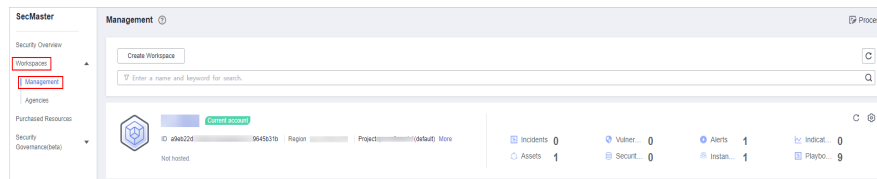
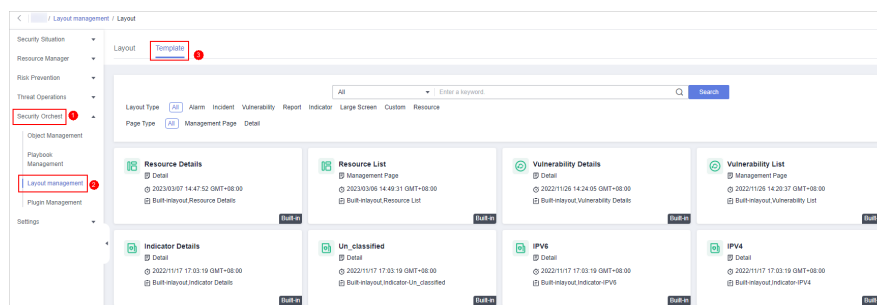
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-131 Management



- Step 4** In the navigation tree on the left, choose **Security Orchestration > Layout Management**. On the Layout Management page, click the **Template** tab.

Figure 11-132 Layout template tab page



- Step 5** On the **Template** tab page, view the template information.

You can search for a specified layout template by **Layout Type** or **Page Type**.

- You can view the name, page type, and creation time of an existing template.
- You can edit the name and layout of an existing template.
- You can delete an existing template.

----End

11.7.2 Manage Existing Layouts

This topic describes how to perform the following operation: [Viewing an Existing Layout](#) and [Deleting a Layout](#).

Viewing an Existing Layout


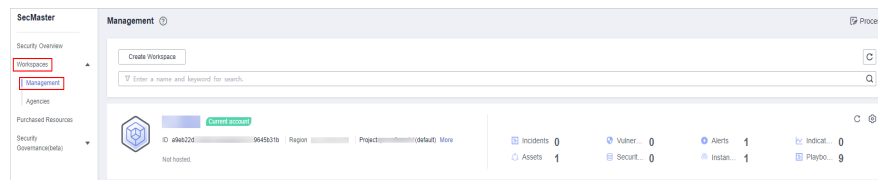
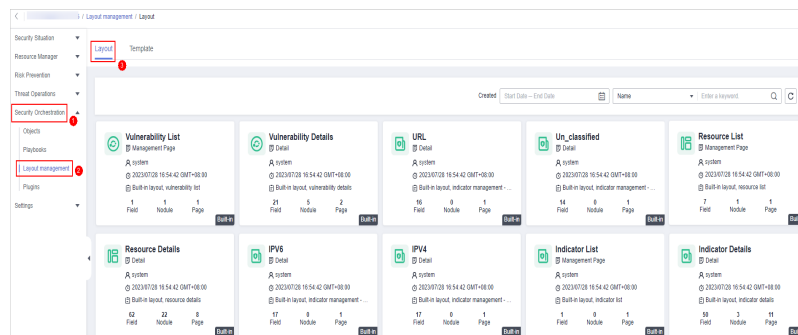
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-133 Management




- Step 4** In the navigation tree on the left, choose **Security Orchestration > Layouts**. The **Layout** tab is displayed by default.

Figure 11-134 Layouts page



- Step 5** On the layout management page, view existing layouts.

Hover your cursor over the target layout and click  in the upper right corner of the layout. The layout configuration details page is displayed.

----End

Deleting a Layout


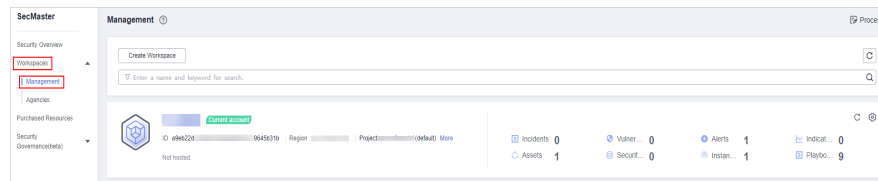
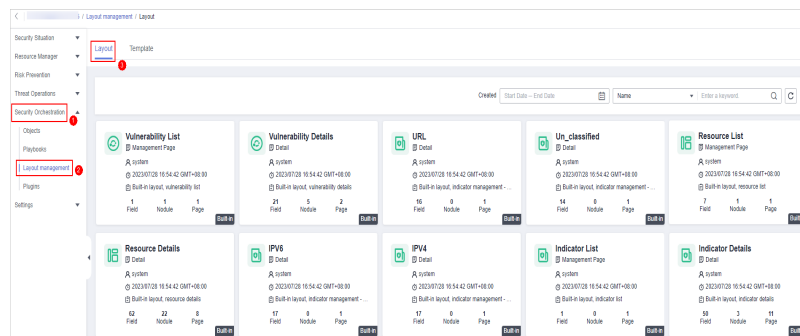
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.


Figure 11-135 Management



Step 4 In the navigation tree on the left, choose **Security Orchestration > Layouts**. The **Layout** tab is displayed by default.

Figure 11-136 Layouts page



Step 5 On the layout management page, move the cursor to a desired layout and click  in the upper right corner of the layout. The deletion confirmation dialog box is displayed.

Step 6 Click **OK**.

----End

11.8 Plug-in Management

11.8.1 Overview

SecMaster supports unified management of plug-ins used in the security orchestration process.

Terms

- **Plug-in:** an aggregation of functions, connectors, and public libraries. There are two types of plug-ins: custom plug-ins and commercial plug-ins. Custom plug-ins can be displayed in marts or used in playbooks.
- **Plug-in set:** a set of plug-ins that have the same service scenario.
- **Function:** an executable function that can be selected in a playbook to perform a specific behavior in the playbook.
- **Connector:** connects to data sources and sends security data such as alerts and incidents to SecMaster. Connectors are classified into incident-triggered connectors and scheduled connectors.
- **Public library:** a public module that contains API calls and public functions that will be used in other components.

11.8.2 Viewing Plug-in Details

This section describes how to view SecMaster built-in plug-ins and their details.

Procedure


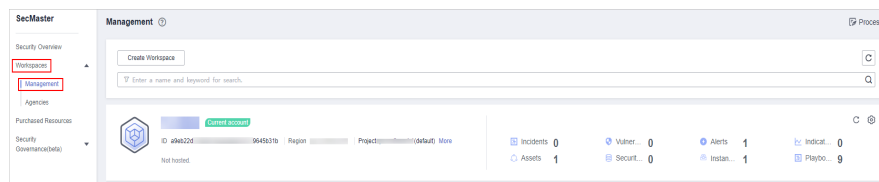
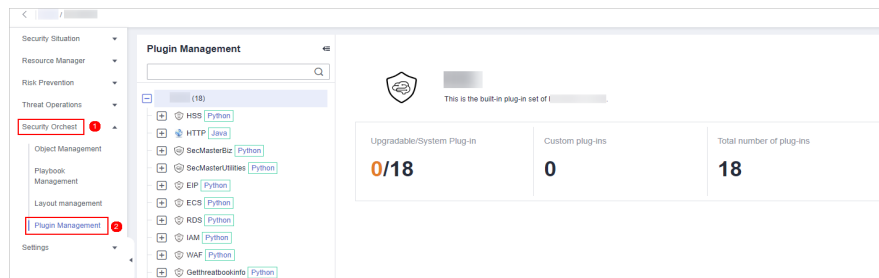
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 11-137 Management



- Step 4** In the navigation pane on the left, choose **Security Orchestration > Plugins**.

Figure 11-138 Plugins page



- Step 5** On the **Plugins** page, view plug-in details.
 - The navigation pane on the left shows information about all built-in plug-in sets, plug-ins, and functions.
 - To view details about a plug-in, click its name. Its details will be displayed in the right pane.
 - To view details about a function, expand the plug-in and click the function name. The function details will be displayed in the right pane.

----End

12 Settings

12.1 Data Collection

12.1.1 Data Collection Overview

Data collection refers to the process of using Logstash to collect varied log data in many methods. After data is collected, historical data analysis and comparison, data association analysis, and unknown threat discovery can be quickly implemented.

Limitations and Constraints

- Currently, the Agent for data collection can run only on Linux hosts running EulerOS of certain versions. For details, see [Supported OSs](#).
- During Agent installation, only IAM accounts can be used for viewing information on the console.

Process

Table 12-1 Data collection process

Procedure		Description
1	Buying an ECS	Purchase an ECS of a specified version.
2	Installing the agent	Install the Agent on the server.
3	Adding a node	Add a collection management node.
4	Configuring components	Configure component information.
5	Adding a data connection	Add a data connection source and destination.

Procedure		Description
6	(Optional) Configuring a parser	Configure a parser to collect data in customized parsing mode.
7	Adding a collection channel	Add a data collection channel.

Supported OSs

Currently, the data collection agent can run only on EulerOS Linux servers on x86_64 architecture. [Table 12-2](#) lists the supported versions.

Table 12-2 Supported EulerOS versions

Version	ECS OS Version
EulerOS 2.5	EulerOS 2.5 64bit for Tenant 20210227 (40GB) EulerOS 2.5 64bit for Tenant 20220321 base 2.5.11 (40GB) EulerOS 2.5 64bit for Tenant 20220906 base 2.5.12 (40GB) EulerOS 2.5 64bit for Tenant 20221130 base 2.5.13 (40GB) Public-CAD-EulerOS-BaseTemplate-2.5.9-x86_64-Standard (dedicated for making resources and not supporting password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.11-x86_64-Standard (dedicated for making resources and not supporting password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.12-x86_64-Standard (dedicated for making resources and not supporting password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.13-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.14-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB)

Version	ECS OS Version
EulerOS 2.9	Public-CAD-EulerOS-BaseTemplate-2.9.6-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.7-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.8-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.9-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.10-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB)
EulerOS 2.10	Public-CAD-EulerOS-BaseTemplate-2.10.5-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.10.6-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.10.7-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB)

12.1.2 Buying an ECS

This topic describes how to purchase an ECS that supports the installation of Agent.

Prerequisites

You have obtained the username and password of an IAM account for logging in to the management console.

Procedure

Purchase an ECS. For details, see the *Elastic Cloud Server User Guide*.

CAUTION

Currently, the data collection agent can run only on EulerOS Linux servers on x86_64 architecture.

Note that you need to select a proper OS and version when you make a purchase. [Table 12-3](#) lists the supported versions.

Figure 12-1 Selecting an OS version

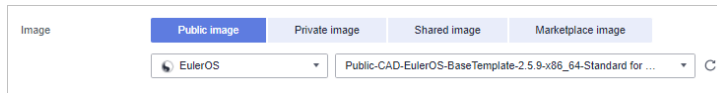


Table 12-3 Supported EulerOS versions

Version	ECS OS Version
EulerOS 2.5	EulerOS 2.5 64bit for Tenant 20210227 (40GB) EulerOS 2.5 64bit for Tenant 20220321 base 2.5.11 (40GB) EulerOS 2.5 64bit for Tenant 20220906 base 2.5.12 (40GB) EulerOS 2.5 64bit for Tenant 20221130 base 2.5.13 (40GB) Public-CAD-EulerOS-BaseTemplate-2.5.9-x86_64-Standard (dedicated for making resources and not supporting password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.11-x86_64-Standard (dedicated for making resources and not supporting password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.12-x86_64-Standard (dedicated for making resources and not supporting password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.13-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.5.14-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB)
EulerOS 2.9	Public-CAD-EulerOS-BaseTemplate-2.9.6-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.7-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.8-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.9.9-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB)

Version	ECS OS Version
	Public-CAD-EulerOS-BaseTemplate-2.9.10-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB)
EulerOS 2.10	Public-CAD-EulerOS-BaseTemplate-2.10.5-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.10.6-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB) Public-CAD-EulerOS-BaseTemplate-2.10.7-x86_64-Standard (dedicated for making resources and not support password injection) (20 GB)

Follow-up Operations

After purchasing an ECS, you need to install the Agent. For details, see [Installing the Agent](#).

12.1.3 Installing the Agent

This topic describes how to install the data collection agent.

Prerequisites

- You have purchased an ECS.
- You have obtained the username and password of an IAM account for logging in to the management console.
- You have completed the following checks before installing the Agent:
 - a. Run the **ps -ef | grep salt** command to check whether the salt-minion process exists on the host.
 - If yes, stop it first.
 - If no, go to **b**.

Figure 12-2 Checking processes

```
[root@host-192-168-... ~]# ps -ef | grep salt
root      18749  18315  0 09:28 pts/0    00:00:00 grep --color=auto salt
root      58881    1  0 Apr11 ?        00:00:00 /usr/bin/python3 /usr/bin/salt-minion
isap-sa+  58888  58881  0 Apr11 ?        00:01:08 /usr/bin/python3 /usr/bin/salt-minion
```

- b. Before installing Logstash, run the **df -h** command to check whether there are at least 50 GB of disk space reserved for the **root** directory disk or **opt** disk, two CPU cores, and 4 GB of memory.

Figure 12-3 Disks

```
[root@ecs- ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1       40G   1.7G   36G   5% /
devtmpfs        7.8G   0    7.8G   0% /dev
tmpfs           7.8G   0    7.8G   0% /dev/shm
tmpfs           7.8G  129M   7.7G   2% /run
tmpfs           7.8G   0    7.8G   0% /sys/fs/cgroup
/dev/vdb1       98G   8.9G   85G  10% /opt
/dev/vdb2      108G   61M  103G   1% /var/lib/docker
tmpfs           1.6G   0    1.6G   0% /run/user/0
```

If the memory is insufficient, stop some applications with high memory usage or expand the memory capacity before the installation.

Procedure


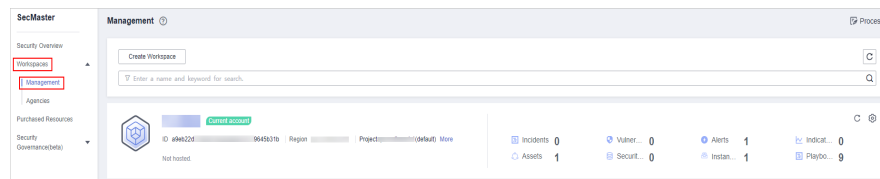
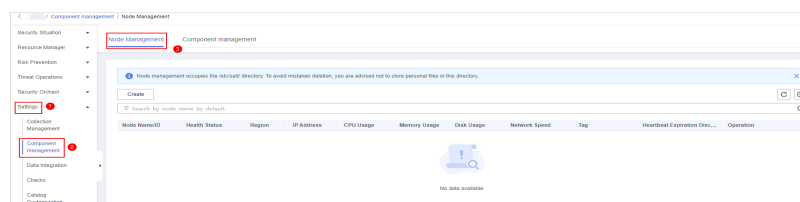
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-4 Management



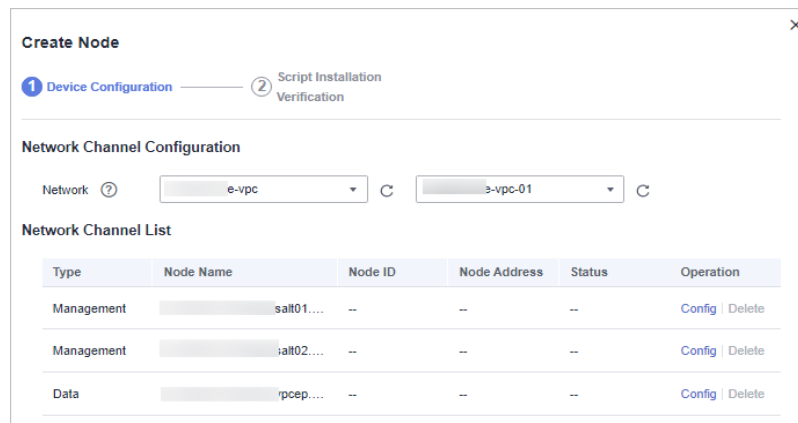
- Step 4** In the navigation tree on the left, choose **Settings > Components**.

Figure 12-5 Node management page




- Step 5** On the **Node Management** page, click **Create**.
- Step 6** On the **Create Node** page, specify parameters.

Figure 12-6 Create Node



1. In the **Network Channel Configuration** area, select the VPC and subnet to which the network channel belongs.
2. In the network channel list, locate the row that contains the target channel and click **Config** in the **Operation** column. In the displayed confirmation dialog box, click **OK**.

Step 7 Click **Next** in the lower right corner of the page. On the page for verifying the script installation, click  to copy the command for installing the Agent.

Step 8 Remotely log in to the ECS where you want to install the Agent.

- You can log in to the ECS management console and click **Remote Login** in the ECS list.
- If your server has an EIP bound, you can also use a remote management tool, such as Xftp, SecureFX, WinSCP, PuTTY, or Xshell, to log in to the server and install the agent on the server as user **root**.

Step 9 Run the `cd /opt/cloud` command to go to the installation directory.

 **CAUTION**

The recommended installation path is `/opt/cloud`. This topic also uses this path as an example. If you want to install the Agent in another path, change the path based on site requirements.

Step 10 Run the command copied in [Step 7](#) as user **root** to install the Agent on the ECS.

Step 11 Enter the IAM username and password for logging in to the console when prompted.

Step 12 If information similar to the following is displayed, the agent is successfully installed:

```
install isap-agent successfully
```

----End

Follow-up Operations

After the Agent is installed, you need to add nodes on the console. For details, see [Creating a Node](#).

Related Operations

[Troubleshooting the Agent Installation Failure](#)

12.1.4 Creating a Node

This topic describes how to create a data collection node.

Prerequisites

The Agent has been installed on the host.

Procedure


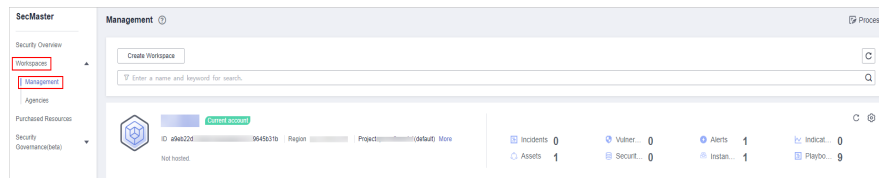
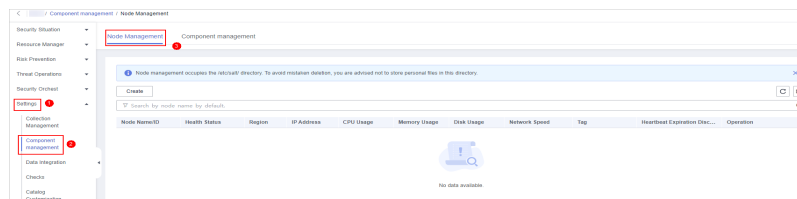
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-7 Management



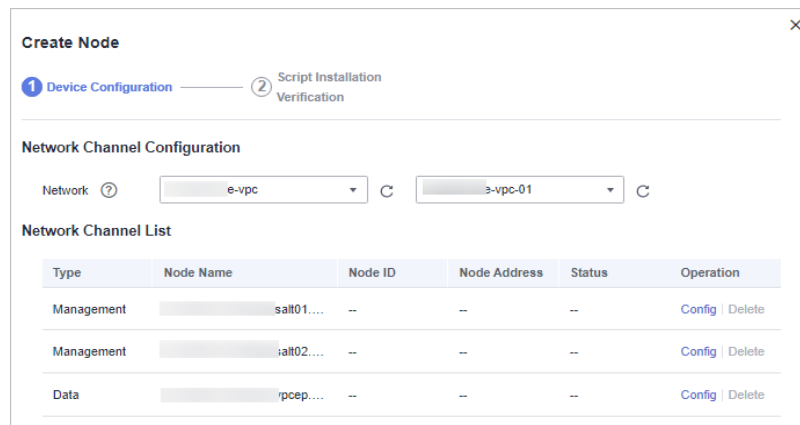
- Step 4** In the navigation tree on the left, choose **Settings > Components**.

Figure 12-8 Node management page



- Step 5** On the **Node Management** page, click **Create**.
- Step 6** On the **Create Node** page, specify parameters.

Figure 12-9 Create Node



1. In the **Network Channel Configuration** area, select the VPC and subnet to which the network channel belongs.
2. In the network channel list, locate the row that contains the target channel and click **Config** in the **Operation** column. In the displayed confirmation dialog box, click **OK**.

Step 7 Click **Next** in the lower right corner of the page to go to the **Script Installation Verification** page.

Step 8 After confirming that the installation is complete, click **Confirm** in the lower right corner of the page.

If it is not installed, rectify the fault by referring to [Installing the Agent](#).

----End

12.1.5 Configuring a Component


This topic describes how to configure a component.

Prerequisites

You have added a node.

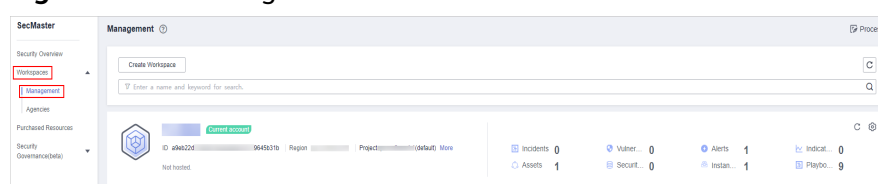
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-10 Management



- Step 4** In the navigation pane on the left, choose **Settings > Components > Component management**.
 - Step 5** On the **Component management** page, click **Edit Configuration** in the upper right corner of the component to be viewed. The configuration management page of the component is displayed on the right.
 - Step 6** In the **Node Configuration** area, click **Add** in the upper left corner of the node list. In the **Adding a Node** dialog box displayed, select a node and click **OK**.
 - Step 7** Click **Save and Apply** in the lower right corner of the page.
- End

Follow-up Operations

After a node is added, you need to add a connection. For details, see [Adding a Connection](#).

12.1.6 Adding a Connection

This topic describes how to add a connection.

Prerequisites

You have configured a component.

Limitations and Constraints

- After a data connection is added, only the parameters of the selected data source type can be modified. The data source type cannot be changed.

Procedure


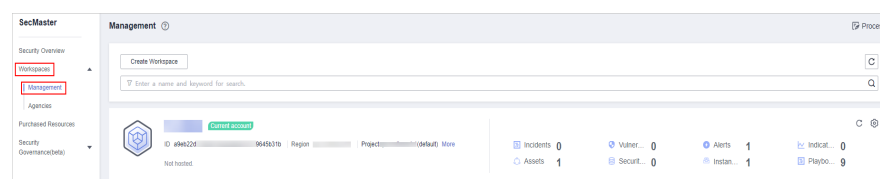
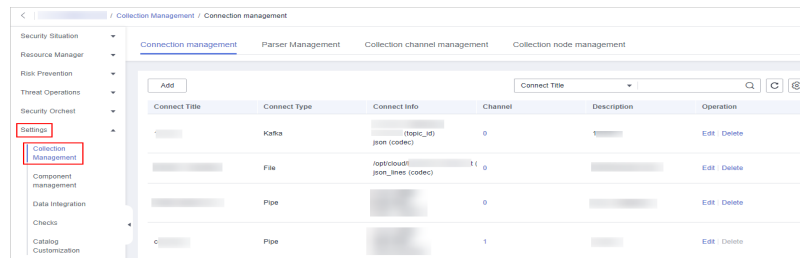
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-11 Management



- Step 4** In the navigation pane on the left, choose **Settings > Collectors**.

Figure 12-12 Collectors page



Step 5 On the **Connection management** page, click **Add**.

Step 6 Add a data connection source.

In the **Source** column, select the source of the data source type and set parameters based on the selected type.

The following data source types are supported: **Transmission Control Protocol (TCP)**, **File**, **User Data Protocol (UDP)**, **Object Storage Service (OBS)**, **Message Queue (Kafka)**, and **SecMaster Pipeline**.

Step 7 Add a data source connection destination.

Click the **Target** tab, select the destination of the data source type, and then set the parameters according to the selected type.

The following data source types are supported: **File**, **Transmission Control Protocol (TCP)**, **User Data Protocol (UDP)**, **Message Queue (Kafka)**, **Object Storage Service (OBS)**, and **SecMaster Pipeline**.

Step 8 After the setting is complete, click **Confirm** in the lower right corner of the page.

----End

Follow-up Operations

After a connection is added, you can configure a parser if needed. For details, see [Configuring a Parser](#).

You can add a collection channel without configuring a parser. For details, see [Adding a Collection Channel](#).

12.1.7 Configuring a Parser

You can use custom parsers to collect data with SecMaster.


This topic describes how to configure a parser.

Prerequisites

A connection has been added by referring to [Adding a Connection](#).

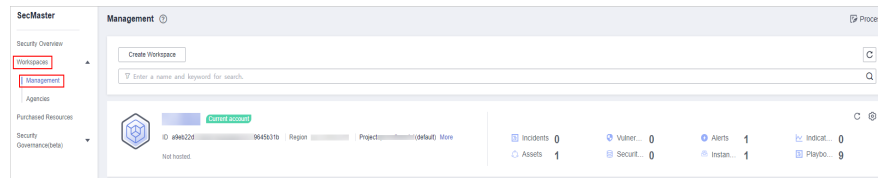
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

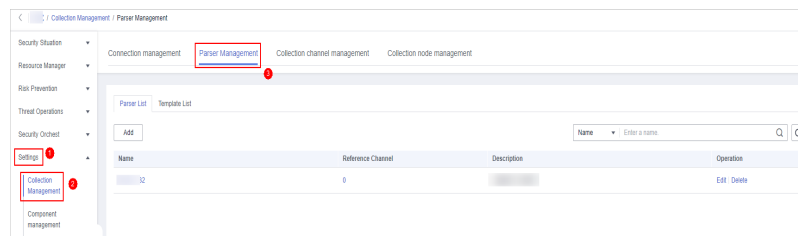
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-13 Management



Step 4 In the navigation pane on the left, choose **Settings > Collectors**. On the displayed page, click the **Parsers** tab.

Figure 12-14 Parser Management tab page



Step 5 [Customize a parser](#) or [create a parser from a template](#).

- **Customizing a parser**
 - a. On the parser management tab page, click **Add**.
 - b. On the **New Parser** page, set parameters.

Table 12-4 Parameters for adding a parser

Parameter		Description
Basic Information	Name	Set a parser name.
	Description	Enter a parser description.
Rule list		Set rules for the parser. Perform the following steps: <ol style="list-style-type: none"> 1. Click Add and select a rule type. <ul style="list-style-type: none"> ○ Parsing rules: Select the parsing rule of the parser. You can select UUID, kv, mutate, grok, date, drop, prune, CSV, or JSON rules. ○ Conditional control: Select the conditions for the parser. You can select If, Else, or Else if. 2. Set parameters based on the selected rule.

- c. Click **OK** in the lower right corner of the page.
- **Creating a Parser from a Template**
 - a. On the **Parser Management** page, click the **Template List** tab.
 - b. On the displayed page, locate the row that contains the target template, click **Create from Template** in the **Operation** column.
 - c. On the **New Parser** page, set parameters.

Table 12-5 Parameters for adding a parser

Parameter		Description
Basic Information	Name	Parser name, which is automatically generated by the system based on the template and can be changed.
	Description	Parser description, which is automatically generated by the system based on the template and can be modified.
Rule list		<p>Parser parsing rule, which is automatically generated by the system based on the template and can be modified.</p> <p>To add a rule, click Add, select a rule type, and set parameters based on the selected rule.</p> <ul style="list-style-type: none"> ▪ Parsing rules: Select the parsing rule of the parser. You can select UUID, kv, mutate, grok, date, drop, prune, CSV, or JSON rules. ▪ Conditional control: Select the conditions for the parser. You can select If, Else, or Else if.

- d. Click **OK** in the lower right corner of the page.

----End

Follow-up Operations

After the parser is configured, you need to add a collection channel. For details, see [Adding a Collection Channel](#).

12.1.8 Adding a Collection Channel

This topic describes how to add a collection channel.

Prerequisites

You have created a connection.

Procedure


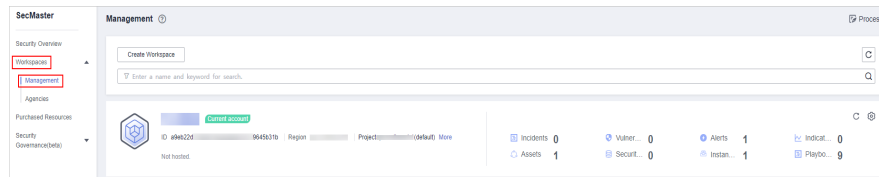
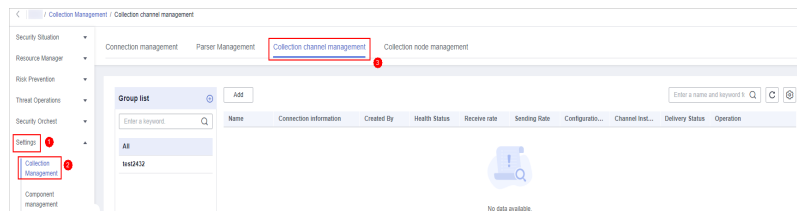
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.



Figure 12-15 Management



- Step 4** In the navigation pane on the left, choose **Settings > Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-16 Collection channel management tab page



- Step 5** Add a channel group.
 1. On the collection channel management page, click  on the right of the **Group list**.
 2. Enter a group name and click .

To edit or delete a group, hover the cursor over the group name and click the edit or deletion icon.

- Step 6** On the right of the group list, click **Add**.
- Step 7** On the displayed page, in the **Basic Configuration** phase, configure basic information.

Table 12-6 Basic configuration parameters

Parameter		Description
Basic Information	Title	User-defined collection channel name.
	Channel grouping	Select the group to which the collection channel belongs.
	Description	Enter the description of the collection channel.

Parameter		Description
Source Configuration	Source Name	Select the source name of the collection channel. After you select a source, the system automatically generates the information about the selected source.
Destination	Destination Name	Select the destination name of the collection channel. After you select a source, the system automatically generates the information about the selected source.

Step 8 After the basic configuration is complete, click **Next** in the lower right corner of the page.

Step 9 On the parser configuration page, select a parser to view its details.

If no parser is available or you want to create a parser, choose **Create** to create a parser. For details, see [Managing Parsers](#).

Figure 12-17 Parser configuration

Step 10 After the parser is configured, click **Next** in the lower right corner of the page.

Step 11 On the **Select Node** page, click **Add**. In the **Add Node** dialog box displayed, select a node and click **Confirm**.

- Running parameters: After a node is added, if you want to configure parameters on the added node, perform the following steps:
 - a. In the node list, locate the row that contains the target node, and click **Running Parameters** in the **Operation** column.
 - b. Click **Add Configuration** and set **Key** and **Value**.
- Removing a node: To remove an added node, locate the row that contains the target node, click **Remove** in the **Operation** column.

Step 12 After the running node is selected, click **Next** in the lower right corner of the page.

Step 13 On the **Channel Details Preview** page, confirm the configuration and click **OK**.

----End

12.1.9 Collection Management

12.1.9.1 Managing Connections


This topic describes how to perform operations of [Viewing Connections](#), [Editing a Data Connection](#), and [Deleting a Data Connection](#).

Limitations and Constraints

- After a data connection is added, only the parameters of the selected data source type can be modified. The data source type cannot be changed.

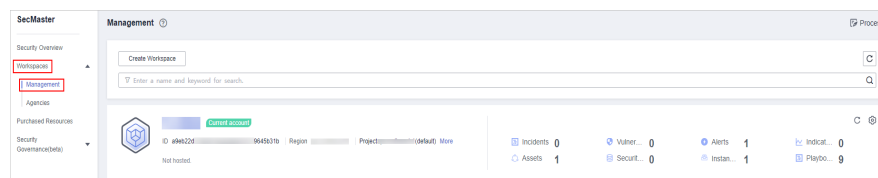
Viewing Connections

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

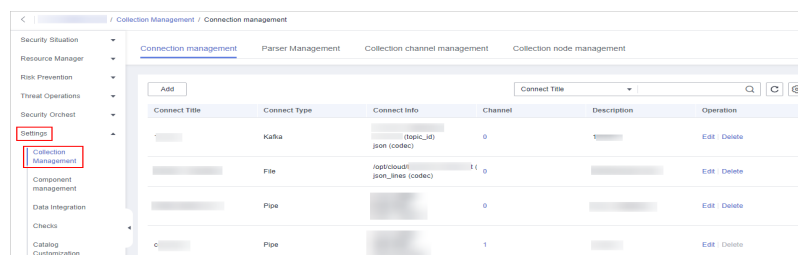
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-18 Management



Step 4 In the navigation pane on the left, choose **Settings > Collectors**.

Figure 12-19 Collectors page



Step 5 On the **Connections** page, view connection details.

Table 12-7 Connection parameters

Parameter	Description
Connection Name	Connection name
Connection Type	Connection type
Connection Info	Information about a connection
Reference Channels	Number of channels that are referenced by the connection
Description	Description of the connection
Operation	Operations such as editing or deleting connections


----End

Editing a Data Connection

NOTE

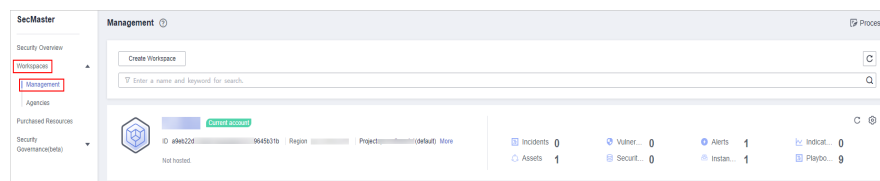
After a data connection is added, only the parameters of the selected data source type can be modified. The data source type cannot be changed. For example, if you select **File** as the data source type when adding a data connection, you can modify only the parameters in the file type but cannot change the **File** type.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

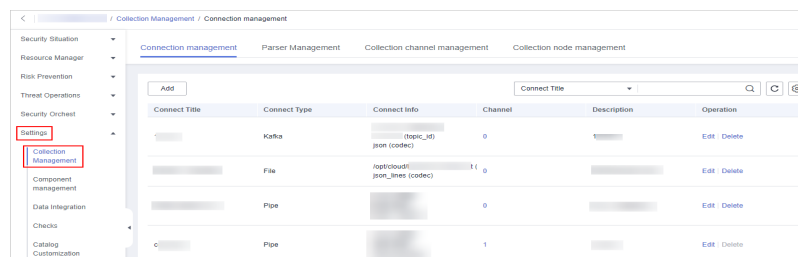
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-20 Management



Step 4 In the navigation pane on the left, choose **Settings > Collectors**.

Figure 12-21 Collectors page



- Step 5** On the Connections page, locate the row that contains the target connection and click **Edit** in the **Operation** column.
 - Step 6** On the **Select Data Source Type** page, edit the parameters of the data source type.
 - Step 7** After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.
- End

Deleting a Data Connection


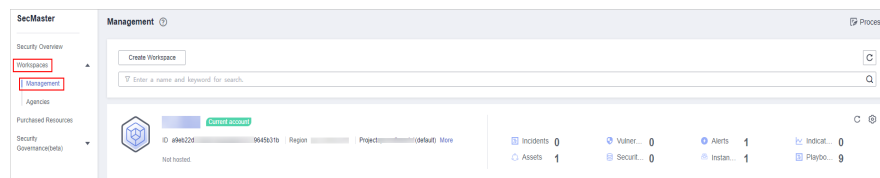
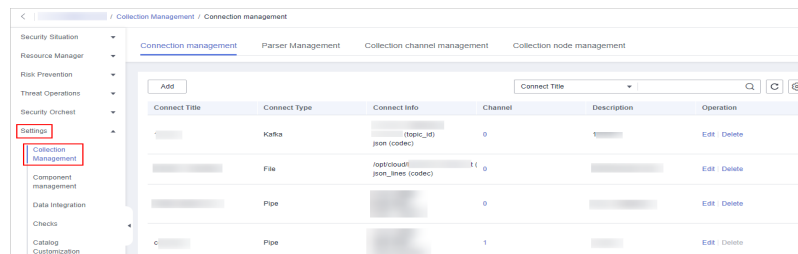
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-22 Management



- Step 4** In the navigation pane on the left, choose **Settings > Collectors**.

Figure 12-23 Collectors page



- Step 5** On the Connections page, locate the row that contains the target connection and click **Delete** in the **Operation** column.
 - Step 6** In the displayed dialog box, click **OK**.
- End

12.1.9.2 Managing Parsers

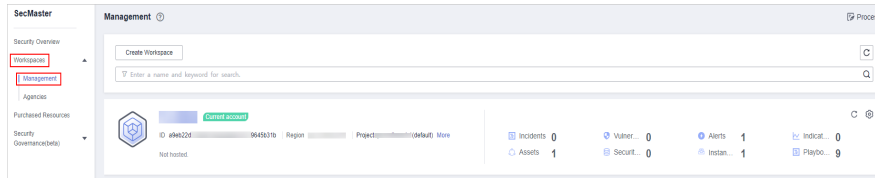
This topic describes how to perform operations of [Viewing Parsers](#), [Editing a Parser](#), and [Deleting a parser](#).

Viewing Parsers

- Step 1** Log in to the management console.

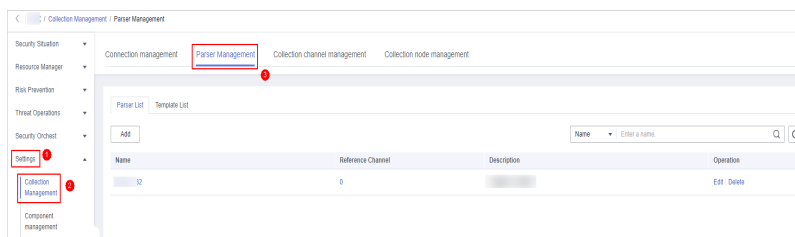
Step 2 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-24 Management



Step 3 In the navigation pane on the left, choose **Settings > Collectors**. On the displayed page, click the **Parsers** tab.

Figure 12-25 Parser Management tab page



Step 4 On the **Parsers** page, view the detailed information about parsers.

Table 12-8 Parsers parameters

Parameter	Description
Parser Name	Name of the parser.
Reference Channels	Number of channels referenced by the parser.
Description	Description of the parser.
Operation	You can edit and delete parsers.

Step 5 On the parser management page, click the **Templates** tab. The **Templates** page is displayed.

Step 6 On the templates page, view the parser template information.

Table 12-9 Parser template parameters

Parameter	Description
Template Name	Name of a parser template
Description	Description of the parser template
Operation	You can create a parser template.

----End

Editing a Parser


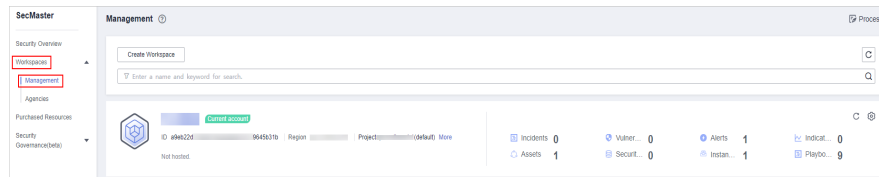
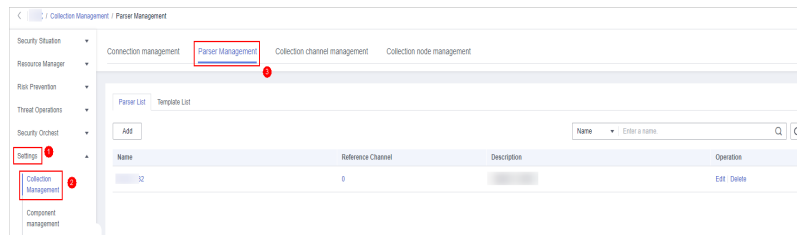
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-26 Management



- Step 4** In the navigation pane on the left, choose **Settings > Collectors**. On the displayed page, click the **Parsers** tab.

Figure 12-27 Parser Management tab page



- Step 5** On the **Parser Management** tab page, locate the row containing your desired parser and click **Edit** in the **Operation** column.
- Step 6** In the **Edit Parser** dialog box, edit the parser information.

Table 12-10 Editing a parser


Parameter		Description
Basic Information	Parser Name	Set the parser name.
	Description	Enter the parser description.
Rules		<p>Set the parsing rule of the parser. Perform the following steps:</p> <p>Click Add and select a rule type.</p> <ul style="list-style-type: none"> ● Parsing Rule: Select the parsing rule of the parser. ● Condition Control: Select the condition control principle of the parser.

Step 7 After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

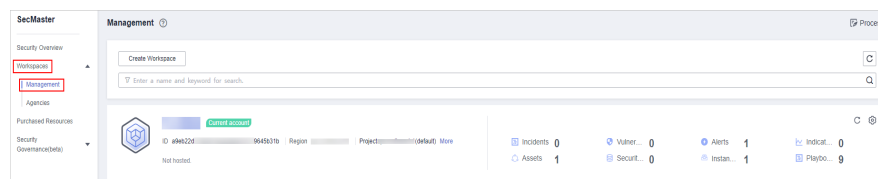
Deleting a parser

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

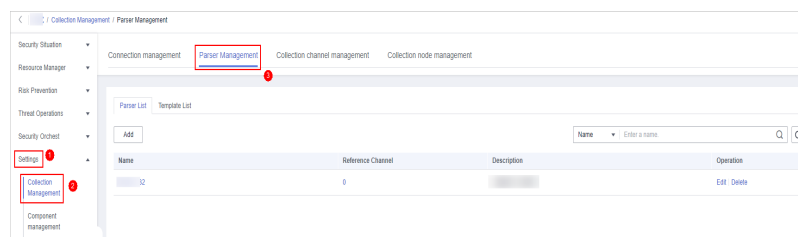
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-28 Management



Step 4 In the navigation pane on the left, choose **Settings > Collectors**. On the displayed page, click the **Parsers** tab.

Figure 12-29 Parser Management tab page



Step 5 On the **Parsers** page, locate the row that contains the target parser and click **Delete** in the **Operation** column.

Step 6 In the displayed dialog box, click **OK**.


----End

12.1.9.3 Managing Collection Channels

This topic describes how to perform operations of [Viewing Collection Channels](#), [Editing a collection channel](#), [Deleting a collection channel](#), and [Enabling/Disabling/Restarting a Collection Channel](#).

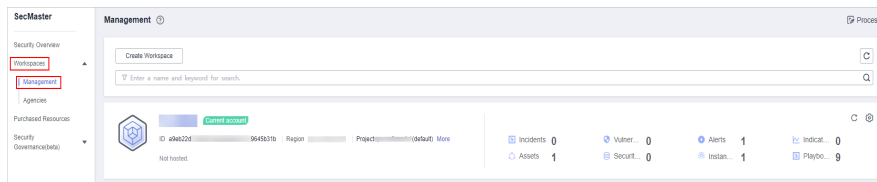
Viewing Collection Channels

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

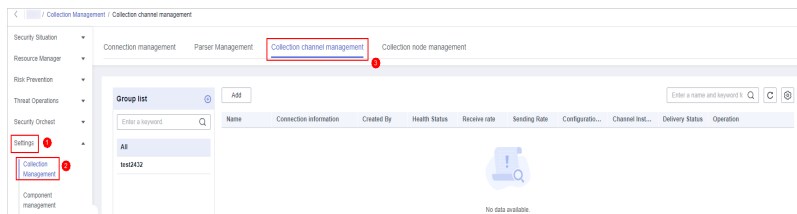
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-30 Management



Step 4 In the navigation pane on the left, choose **Settings > Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-31 Collection channel management tab page



Step 5 On the **Collection Channels** page, view the detailed information about collection channels.


Table 12-11 Collection channel parameters

Parameter	Description
Channel Groups	List of collection channel groups and group names.
Channel Name	Name of the collection channel.
Connection Information	Collect channel connection information
Created By	Creator of the collection channel
Health Status	Health status of the collection channel
Receive Rate	Receive rate of the collection channel
Transmit Rate	Transmit rate of the collection channel
Configuration Status	Configuration status of the collection channel
Channel Instances	Number of collection channels
Running Status	Running status of a collection channel
Operation	You can edit and stop collection channels.

----End

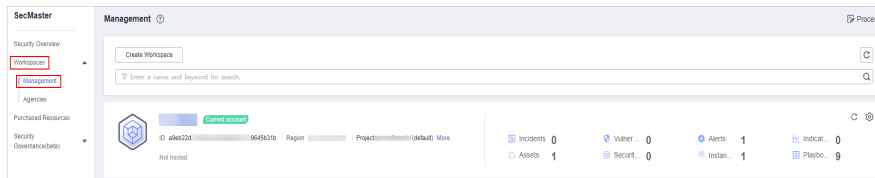
Editing a collection channel

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

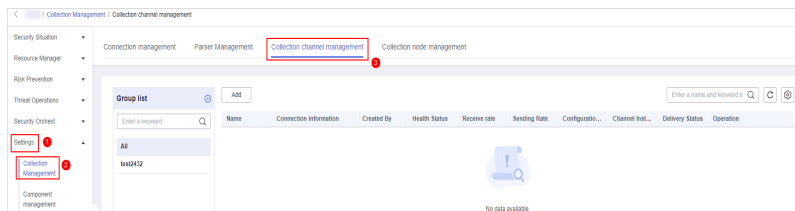
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-32 Management



Step 4 In the navigation pane on the left, choose **Settings > Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-33 Collection channel management tab page



Step 5 In the collection channel list, locate the row that contains the target channel, click **More > Edit** in the **Operation** column. The **Edit Collection Channel** page is displayed.

Step 6 On the displayed page, in the **Basic Configuration** phase, configure basic information.

Figure 12-34 Basic Configuration

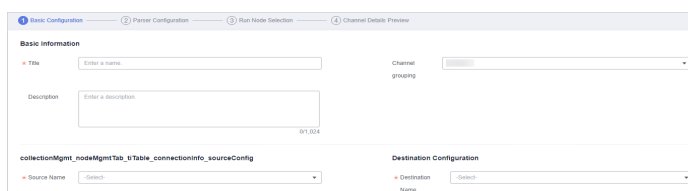


Table 12-12 Basic configuration parameters

Parameter		Description
Basic Information	Channel Name	User-defined collection channel name.
	Channel grouping	Select the group to which the collection channel belongs.
	Description	(Optional) Enter the description of the collection channel.

Parameter		Description
Source Configuration	Source Name	Select the source name of the collection channel. After you select a source, the system automatically generates the information about the selected source.
	Destination Name	Select the destination name of the collection channel. After you select a destination, the system automatically generates the information about the selected destination.

Step 7 After the basic configuration is complete, click **Next** in the lower right corner of the page.

Step 8 On the parser configuration page, select a parser to view its details.

If no parser is available or you want to create a parser, choose **Create** to create a parser. For details, see [Managing Parsers](#).

Figure 12-35 Parser configuration

Step 9 After the parser is configured, click **Next** in the lower right corner of the page.

Step 10 On the **Select Node** page, click **Add**. In the **Add Node** dialog box displayed, select a node and click **Confirm**.

- Running parameters: After a node is added, if you want to configure parameters for the added node, perform the following steps:
 - a. In the node list, locate the row that contains the target node, and click **Running Parameters** in the **Operation** column.
 - b. Click **Add Configuration** and set **Key** and **Value**.
- Removing a node: To remove an added node, locate the row that contains the target node, click **Remove** in the **Operation** column.

- Step 11** After the running node is selected, click **Next** in the lower right corner of the page.
 - Step 12** On the **Channel Details Preview** page, confirm the configuration and click **OK**.
- End

Deleting a collection channel


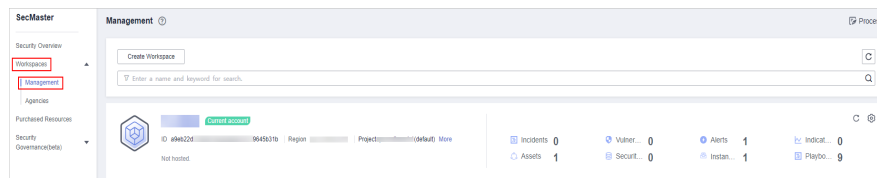
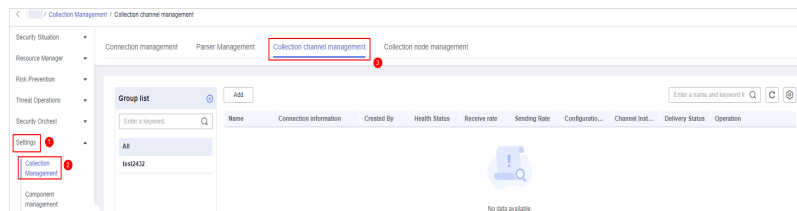
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-36 Management



- Step 4** In the navigation pane on the left, choose **Settings > Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-37 Collection channel management tab page



- Step 5** In the collection channel list, locate the row that contains the target channel, click **More > Delete** in the **Operation** column.

NOTE

You can delete a collection channel only when it is stopped.

- Step 6** In the displayed dialog box, click **OK**.

----End

Enabling/Disabling/Restarting a Collection Channel


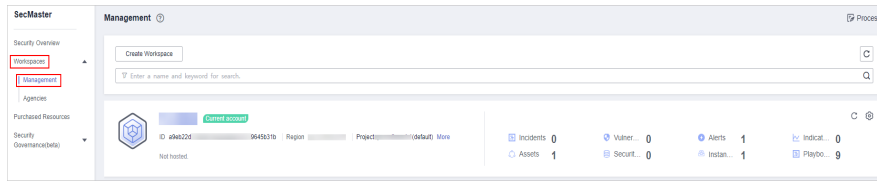
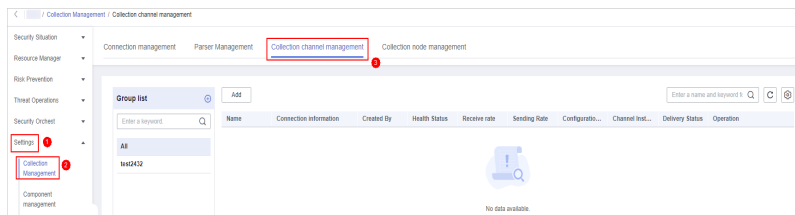
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-38 Management



Step 4 In the navigation pane on the left, choose **Settings > Collection Management**. On the **Collection Management** page, click the **Collection Channels** tab.

Figure 12-39 Collection channel management tab page



Step 5 In the collection stream management list, locate the row that contains the target stream and click **Enable**, **Stop**, or **Restart** in the **Operation** column.

Step 6 In the displayed dialog box, click **OK**.


----End

12.1.9.4 Managing Collection Nodes

This topic describes how to perform the operation of **Viewing Collection Nodes**.

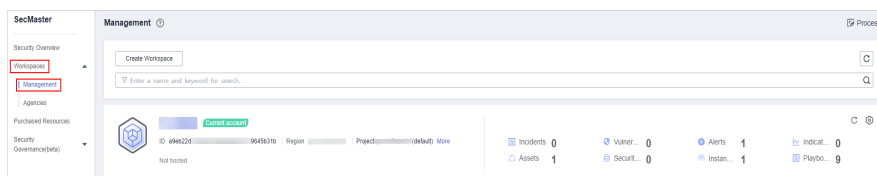
Viewing Collection Nodes

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

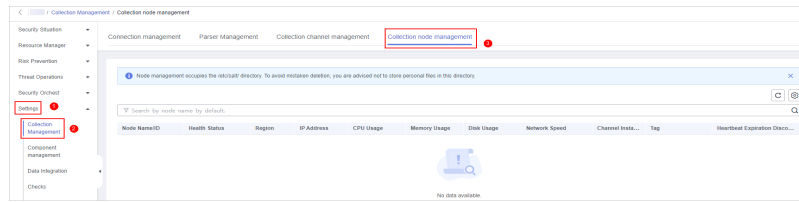
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-40 Management



Step 4 In the navigation pane on the left, choose **Settings > Collection Management**. On the Collection Management page, click the **Collection Nodes** tab.

Figure 12-41 Collection node management tab page



Step 5 On the **Collection Nodes** page, view the detailed information about collection nodes.


If there are a large number of nodes, you can select **Node Name** or **Node ID**, enter a keyword in the search box, and click  to quickly search for a specified node.

Table 12-13 Collection node parameters

Parameter	Description
Node Name/ID	Name or ID of a node
Health Status	Node health status
Region	Region where the node is located
IP Address	Node IP address
CPU Usage	CPU usage of the node
Memory Usage	Memory usage of the node
Disk Usage	Node disk usage
Network Speed	Network rate of a node
Label	Label information of a node
Heartbeat Expiration Mark	Indicates whether the node is disconnected due to heartbeat expiration.

Step 6 To view details about a node, click the node name.

----End


12.1.10 Component Management

12.1.10.1 Managing Collection Nodes

This topic describes how to perform operations such as [Viewing Nodes](#), [Editing a node](#), and [Deregistering a Node](#).

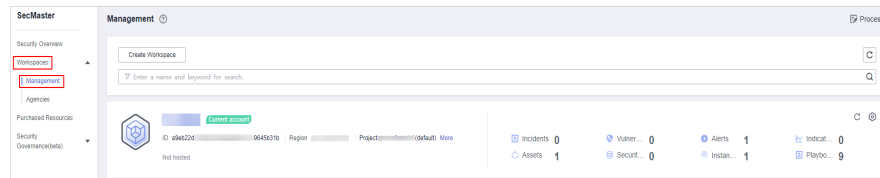
Viewing Nodes

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

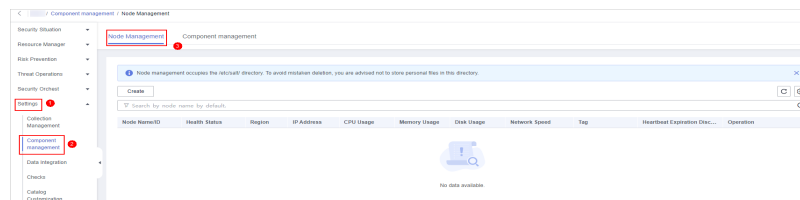
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-42 Management



Step 4 In the navigation tree on the left, choose **Settings > Components**.

Figure 12-43 Node management page



Step 5 On the **Nodes** page, view the detailed information about nodes.


If there are a large number of nodes, you can select **Node Name** or **Node ID**, enter a keyword in the search box, and click  to quickly search for a specified node.

Table 12-14 Collection node parameters

Parameter	Description
Node Name/ID	Name or ID of a node
Health Status	Node health status
Region	Region where the node is located
IP Address	Node IP address
CPU Usage	CPU usage of the node
Memory Usage	Memory usage of the node
Disk Usage	Node disk usage
Network Speed	Network rate of a node
Label	Label information of a node
Heartbeat Expiration Mark	Indicates whether the node is disconnected due to heartbeat expiration.


Step 6 To view details about a node, click the node name.

----End

Editing a node

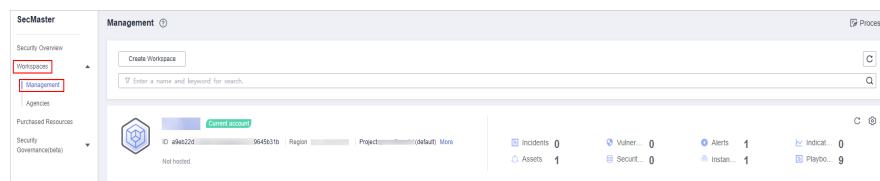
After a node is added, you can only modify the supplementary information about the node.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

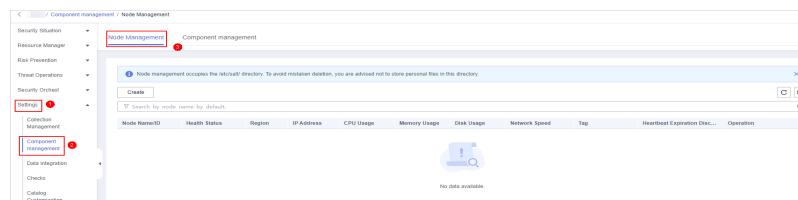
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-44 Management



Step 4 In the navigation tree on the left, choose **Settings > Components**.

Figure 12-45 Node management page



Step 5 On the node management page, locate the row that contains the target node, click **Edit** in the **Operation** column.

Step 6 On the **Edit Node** page, edit the supplementary information about the node.

Table 12-15 Parameters of supplementary node information


Parameter	Description
Data Center	User-defined data center name
Network Plane	Select the network plane of the node.
Label	Set the label of the node.
Description	Description of a user-defined node.
Owner	Select a node owner.

Step 7 Click **OK**.

----End

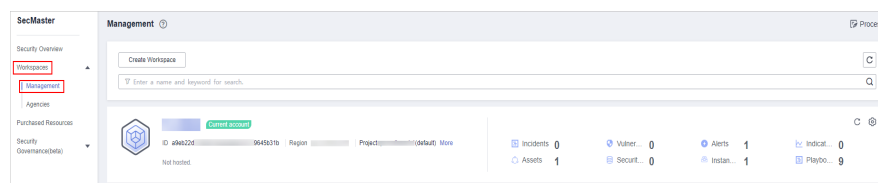
Deregistering a Node

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

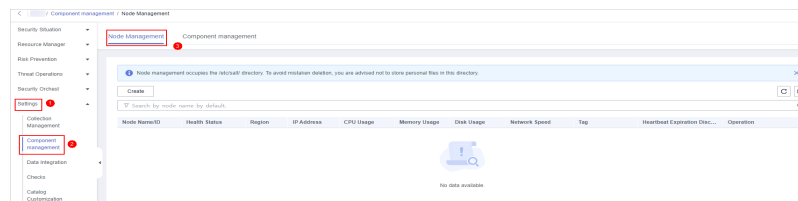
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-46 Management



Step 4 In the navigation tree on the left, choose **Settings > Components**.

Figure 12-47 Node management page



Step 5 On the **Nodes** page, locate the row that contains the target node and click **Deregister** in the Operation column.

Step 6 In the displayed dialog box, click **OK**.

NOTE

Only the node is deregistered. The ECS and endpoint interface resources are not deleted.


----End

12.1.10.2 Managing Components

This topic describes how to view component information.

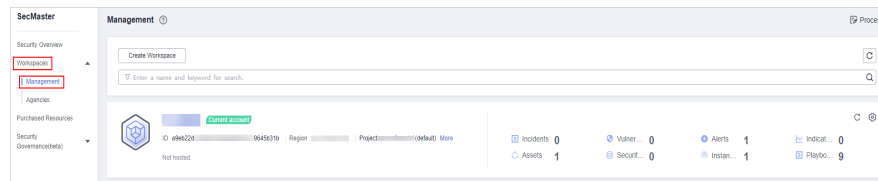
Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-48 Management



Step 4 In the navigation pane on the left, choose **Settings > Components > Components**.

Step 5 On the **Components** page, view the component details.

- **Running node:**
 - Click the **Running Node** in the upper right corner of a component. The running node information of the component is displayed on the right.
- **Checking the configuration:**
 - Click **View Configuration** in the upper right corner of the component to be viewed. The detailed configuration information of the component is displayed on the right.
- **Editing the configuration:**
 - a. Click **Edit Configuration** in the upper right corner of the component to be viewed. The configuration page of the component is displayed on the right.
 - b. In the **Node Configuration** area, edit the node configuration information.
 - Adding a node: Click **Add** in the upper left corner of the node list. In the **Add Node** dialog box that is displayed, select a node and click **OK**.
 - To edit the parameters of an added node, click **▼** next to the node name to expand the node configuration information and edit the node parameters.
 - Running Parameter: Locate the row that contains the target node, click **Parameter** in the **Operation** column.
 - Removing a node: Locate the row that contains the target node and click **Remove** in the **Operation** column.
 - Batch deletion: Select the nodes to be removed and click **Batch Remove** in the upper left corner of the list.
 - To view historical versions, click **Historical Versions** at the lower right corner of the page.
 - c. Click the **Apply** at the lower right corner of the page.

----End


12.2 Data Integration

12.2.1 Access Data

SecMaster can integrate logs of multiple cloud products. You can search for and analyze all collected logs in SecMaster.

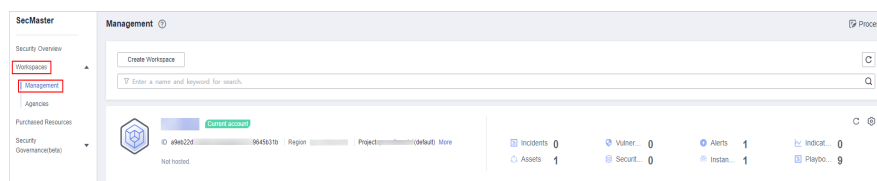
Allowing SecMaster to Access Service Logs

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

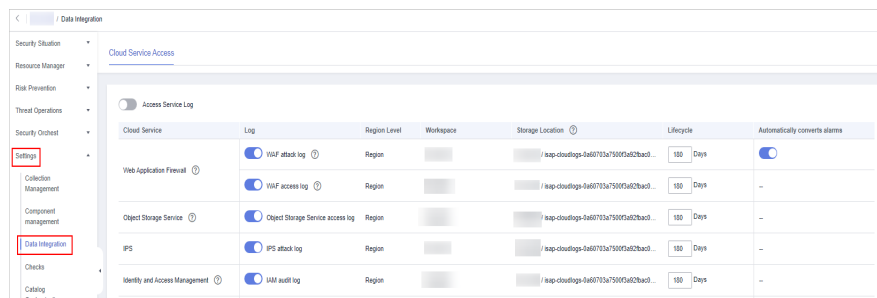
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.


Figure 12-49 Management




Step 4 In the navigation pane on the left, choose **Settings > Data Integration**.

Figure 12-50 Data Integration page




Step 5 Locate the cloud service from which you want to collect logs, click  in the **Log** column to enable log access.

To access logs of all cloud services in the current region, click  on the left of **Access Service Log**.

Step 6 Set the lifecycle.

By default, data is stored for 7 days. You can set the storage period as required.

Step 7 Set **Automatically converts alarms**.

In the **Automatically converts alarms** column of your desired cloud products, click  to enable the function of automatically converting cloud service logs to alerts when the logs meet certain alert rules and displaying the alerts on the **Alerts** page.

 **NOTE**

- If this function is disabled, logs that meet certain alert rules will not be converted to alerts or displayed on the **Alerts** page.
- You can access host vulnerability scan results on the **Vulnerabilities** page of SecMaster. If such results have been accessed during data integration but this conversion function is disabled, the results will not be displayed on the **Vulnerabilities** page.


Step 8 Click **Save**.

After the access completes, a default data space and pipeline are created.

----End

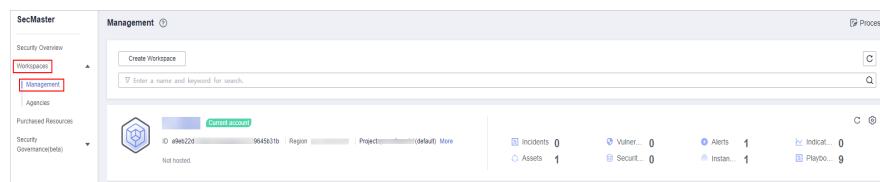
Viewing the Log Storage Location

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-51 Management





Step 4 In the navigation tree on the left, choose **Settings > Data Integration**. On the displayed **Cloud Service Access** tab, view the log data storage location in the **Storage Location** column.

You can go to the corresponding pipeline in the target workspace to view the accessed logs.

----End

Related Operations

- Canceling Data Access
 - In the **Log** column of the target cloud services, click  to disable the access to cloud service logs.
 - Click **Save**.
- Editing the Data Access Lifecycle
 - In the **Lifecycle** column of the target cloud services, enter the data storage period.
 - Click **Save**.
- Canceling Automatic Converting Logs to Alarms
 - In the **Automatically converts alarms** column of the target cloud products, click  to disable the alarms.

- b. Click **Save**.

12.3 Checks

This topic describes how to create baseline check plans. To use cloud service baseline inspection, you need to create check plans first.

Procedure


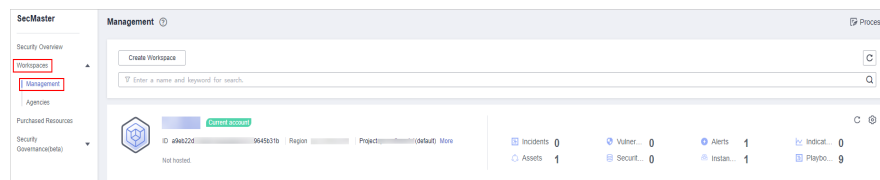
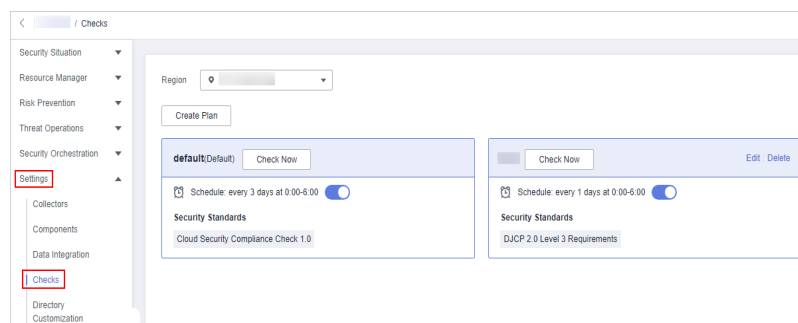
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-52 Management



- Step 4** In the navigation pane on the left, choose **Settings > Checks**.

Figure 12-53 Checks page



- Step 5** On the **Checks** page, click **Create Plan**. The pane for creating a check plan is displayed on the right.

- Step 6** Configure the check plan.

1. Enter the basic information by referring to [Table 12-16](#).

Table 12-16 Basic information about a check plan

Parameter	Description
Name	Plan name

Parameter	Description
Schedule	<p>Select how often and when the check plan is executed.</p> <ul style="list-style-type: none"> - Schedule: every day, every 3 days, every 7 days, every 15 days, or every 30 days - Check start time: 00:00-06:00, 06:00-12:00, 12:00-18:00, or 18:00-24:00

2. Select a security standard for the plan.
Select the baseline check items to be checked.

Step 7 Click **OK**.

After the check plan is created, SecMaster performs cloud service baseline scanning at the specified time. You can choose **Risk Prevention > Baseline Check** to view the scanning result.

----End

12.4 Customizing Directories

You can customize directories on SecMaster. This section includes the following content:


- [Viewing Existing Directories](#)
- [Changing Layout](#)

Limitations and Constraints

- Built-in directories **cannot** be edited or deleted.

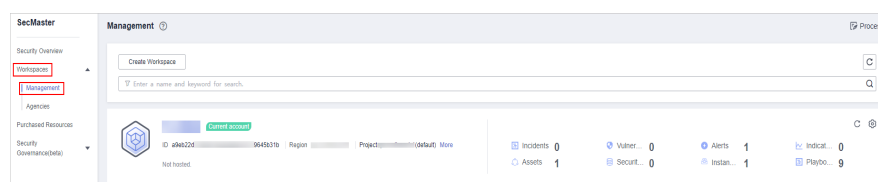
Viewing Existing Directories

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

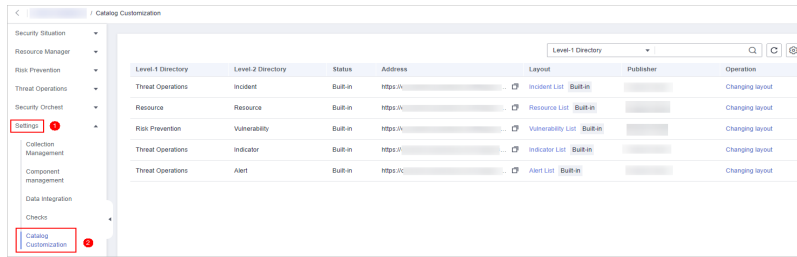
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-54 Management



Step 4 In the navigation tree on the left, choose **Settings > Directory Customization**.

Figure 12-55 Directory Customization page



Step 5 In the directory list, view the directory details.


Table 12-17 Directory parameters

Parameter	Description
Level-1 Directory	Name of the level-1 directory to which the directory belongs
Level-2 Directory	Name of the level-2 directory to which the directory belongs
Status	Type of the directory.
Address	Address of the directory.
Layout	Layout associated with the directory.
Publisher	Publisher of the directory.
Operation	Operations you can do for the directory, such as changing the layout.

----End

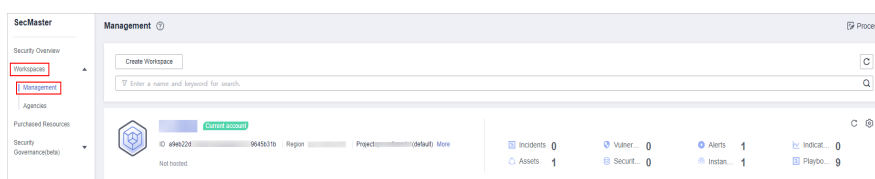
Changing Layout

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

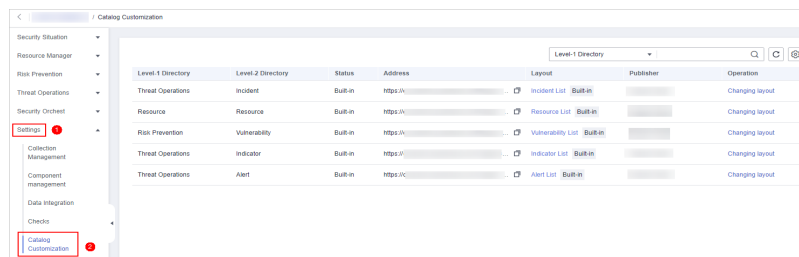
Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 12-56 Management



Step 4 In the navigation tree on the left, choose **Settings > Directory Customization**.

Figure 12-57 Directory Customization page



Step 5 Click **Changing layout** in the **Operation** column of the target directory.

Step 6 On the **Changing layout** page, select the layout to be changed.

Step 7 Click **OK**.

----End

13 Permissions Management

13.1 Creating a User and Granting Permissions

You can use **IAM** to implement fine-grained permission control for your SecMaster resources. With IAM, you can

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing SecMaster resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or cloud service to perform professional and efficient O&M on your SecMaster resources.

If your account does not require individual IAM users, skip over this section.

The following walks you through how to grant permissions. **Figure 13-1** shows the process.

Prerequisites

Learn about the permissions supported by SecMaster and choose policies or roles according to your requirements.

Table 13-1 lists all the system-defined roles and policies supported by SecMaster.

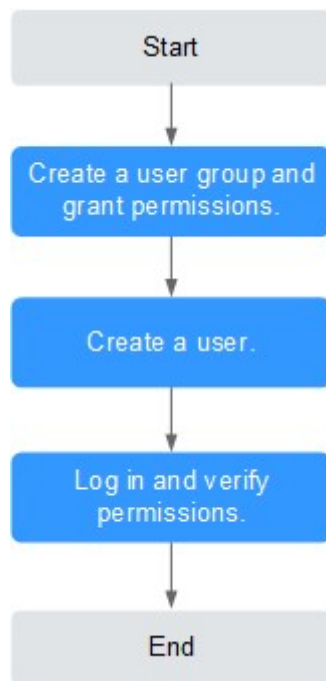
Table 13-1 System-defined permissions supported by SecMaster

Policy Name	Description	Type	Dependency
SecMaster FullAccess	All permissions of SecMaster.	System-defined policy	None

Policy Name	Description	Type	Dependency
SecMaster ReadOnlyAccess	SecMaster read-only permission. Users granted with these permissions can only view SecMaster data but cannot configure SecMaster.	System-defined policy	None

Permission Granting Process

Figure 13-1 Process for granting permissions



1. **Create a user group and assign permissions.**
Create a user group on the IAM console, and assign the **SecMaster FullAccess** permission to the group.
2. **Create a user and add the user to the user group.**
Create a user on the IAM console and add the user to the group created in 1.
3. Log in to the SecMaster console as the created user, and verify that the user only has read permissions for SecMaster.
Choose any other service from **Service List**. If a message appears indicating that you do not have permissions to access the service, the **SecMaster FullAccess** policy has already taken effect.

13.2 SecMaster Custom Policies

Custom policies can be created to supplement the system-defined policies of SecMaster. For the actions that can be added to custom policies, see [SecMaster Permissions and Supported Actions](#).

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see [Creating a Custom Policy](#). The following section shows examples of common SecMaster custom policies.

Example Custom Policies

- Example 1: Authorization for alert list search permission and permission execution analysis

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secmaster:alert:list",
        "secmaster:search:createAnalysis"
      ]
    }
  ]
}
```

- Example 2: Preventing users from modifying alert configurations

A deny policy must be used together with other policies. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

The following method can be used to create a custom policy to disallow users who have the **SecMaster FullAccess** policy assigned to modify alert configurations. Assign both **SecMaster FullAccess** and the custom policies to the group to which the user belongs. Then the user can perform all operations except modifying alert configurations on SecMaster. The following is an example of a deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "secmaster:alert:updateType"
      ]
    }
  ]
}
```

- Example 3: Defining permissions for multiple services in a policy

A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secmaster:alert:get",
        "secmaster:alert:update"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "hss:vuls:set",
        "hss:vuls:list"
      ]
    }
  ]
}
```

13.3 SecMaster Permissions and Supported Actions

This topic describes fine-grained permissions management for your SecMaster. If your account does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

Permissions are classified into roles and policies based on the authorization granularity. A role is a coarse-grained authorization mechanism provided by IAM to define permissions based on users' job responsibilities. A policy defines permissions required to perform operations on specific cloud resources under certain conditions. IAM uses policies to perform fine-grained authorization.

Supported Actions

SecMaster provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- **Permission:** A statement in a policy that allows or denies certain operations.
- **Action:** Specific operations that are allowed or denied.

14 FAQs

14.1 Product Consulting

14.1.1 What Is SecMaster?

SecMaster is a next-generation cloud native security operation platform. It enables integrated and automatic security operations through cloud asset management, security posture management, security information and incident management, security orchestration and automatic response, cloud security overview, simplified cloud security configuration, configurable defense policies, and intelligent and fast threat detection and response.

14.1.2 Why Is There No Attack Data or Only A Small Amount of Attack Data?

SecMaster can detect a variety of attacks on cloud assets and presents them objectively. If your assets are exposed to little risks, such as port exposure and weak passwords, on the Internet, the attack possibility will greatly reduce and there will be no or little data on SecMaster.

14.1.3 What Are Data Sources of SecMaster?

Based on the threat data collected from the cloud and other services, SecMaster analyzes and displays the threat posture through big data mining and machine learning, and provides protection suggestions.

- SecMaster presents overall security posture and generates threat alerts by obtaining network-wide traffic data and logs of security protection devices and using AI and big data technologies to analyze the obtained data.
- Additionally, SecMaster aggregates alarm data from other security services, such as Host Security Service (HSS) and Web Application Firewall (WAF). Based on obtained data, SA then performs big data mining, machine learning, and intelligent AI analysis to identify attacks and intrusions, helping you understand the attack and intrusion processes and providing related protection suggestions.

By analyzing security data that covers every aspect of your services, SecMaster makes it easier for you to understand comprehensive security situation of your services and make informed decisions and handle security incidents in real time.

14.1.4 What Are the Dependencies and Differences Between SecMaster and Other Security Services?

SecMaster can work with other security services such as WAF, HSS, Anti-DDoS, and DBSS.

- **How SecMaster Works With Other Services**

SecMaster is a security management service that depends on other security services to provide threat detection data so that it can analyze security threat risks, display the global security threat posture, and provide informed suggestions.

Other security services report detected threats to SecMaster and SecMaster aggregates the received data to display the global security posture.

- **Differences Between SecMaster and Other Security Services**

SecMaster: It is only a visualized threat detection and analysis platform and does not implement any specific protective actions. It must be used together with other security services.

Other security services display the event data detected by themselves only. They can take specific protective actions, but cannot display global threat posture.

Table 14-1 describes the differences between SecMaster and other security protection services.

Table 14-1 Differences between SecMaster and other services

Service	Category	Dependency and Difference	Protected Object
SecMaster	Security management	SecMaster focuses on the global security threat and attack situation, analyzes threat data generated by several security services and cloud security threats, and provides protection suggestions.	Display the global security threat attack situation.
Anti-DDoS	Network security	Anti-DDoS detects and defends against abnormal DDoS attack traffic, and synchronizes attack logs and defense data to SecMaster.	Ensure enterprise service stability.
HSS	Host security	HSS detects host security risks, executes protection policies, and synchronizes related alerts and protection data to SecMaster.	Ensures host security.

Service	Category	Dependency and Difference	Protected Object
WAF	Application security	WAF detects and protects website service traffic in multiple dimensions to defend against common attacks and block threats. Intrusion logs and alert data are synchronized to SecMaster to present the network-wide web risk situation.	Ensure availability and security of web applications.
DBSS	Data security	DBSS protects and audits database access behaviors. Related audit logs and alert data are synchronized to SecMaster.	Ensure the security of databases and assets on the cloud.

14.1.5 What Are the Differences Between SecMaster and HSS?

Service Positioning

- SecMaster is a next-generation cloud native security operations platform. It enables integrated and automatic security operations through cloud asset management, security posture management, security information and incident management, security orchestration and automatic response, cloud security overview, simplified cloud security configuration, configurable defense policies, and intelligent and fast threat detection and response.
- Host Security Service (HSS) is designed to protect server workloads in hybrid clouds and multi-cloud data centers. It protects servers and containers and prevents web pages from malicious modifications.

In short, SecMaster presents the comprehensive view of security posture, and HSS secures servers and containers.

Function Differences

- SecMaster collects security data (including detection data of security services such as HSS, WAF, and Anti-DDoS) on the entire network and provides capabilities such as cloud asset management, security posture management, security information and incident management, security orchestration, and automatic response, helping you implement integrated and automatic security operations management.
- HSS uses technologies such as AI, machine learning, and deep algorithms to analyze server risks through agents installed on protected servers. It delivers inspection and protection tasks through the console. You can manage the security information reported by the Agent through the HSS console.

Table 14-2 Differences between SecMaster and HSS

Item		Common Function	Difference
Asset security	Server	Both can display the overall security posture of servers.	<ul style="list-style-type: none"> • SecMaster synchronizes server risk data from HSS and then displays overall server security posture. • HSS scans accounts, ports, processes, web directories, software information, and automatic startup tasks on servers and displays server security posture.
	Websites	-	<ul style="list-style-type: none"> • SecMaster checks and scans the overall security posture of website assets from different dimensions. • HSS does not support this function.
Vulnerability	Server vulnerabilities	Both can display server scanning results and support server vulnerability management.	<ul style="list-style-type: none"> • SecMaster synchronizes server vulnerability data from HSS and allows you to manage server vulnerabilities in SecMaster. • HSS allows you to manage Linux, Windows, Web-CMS, and application vulnerabilities. It also gives you an overview of vulnerabilities in real time, including vulnerability scan details, vulnerability statistics, vulnerability types and distributions, your top 5 vulnerabilities, and the top 5 risky servers.
	Website vulnerabilities	-	<ul style="list-style-type: none"> • SecMaster synchronizes website vulnerability scan results from HSS so you can manage these vulnerabilities in SecMaster. • HSS does not support this function.
Baseline inspection	Cloud service baseline	-	<ul style="list-style-type: none"> • SecMaster can help you check key configurations of cloud services you enabled based on built-in checks. • HSS does not support this function.
	Unsafe settings	-	<ul style="list-style-type: none"> • SecMaster does not support this function. • HSS checks your baseline settings, including checking for weak passwords, and reviewing security policies and configuration details. HSS provides an overview of your configuration security rating, the top 5 configuration risks, detected weak passwords, and the top 5 servers with weak passwords configured.

14.1.6 How Do I Update My Security Score?

SecMaster checks your asset health in real time, evaluates the overall security posture, and gives a security score. A security score helps you quickly understand the overall status of unprocessed risks to your assets.

After asset security risks are fixed, manually ignore or handle alerts and update the alert status in the alert list. The risk severity can be down to a proper level accordingly. Your security score will be updated after you refresh the alert status and check your environment again.

Procedure


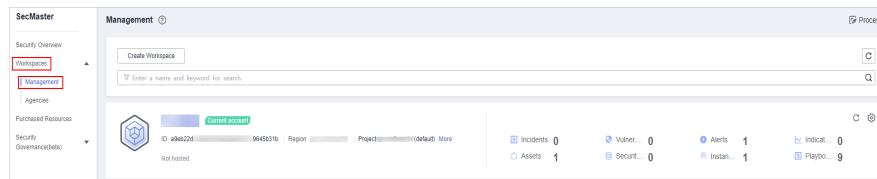
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 14-1 Management



- Step 4** In the navigation tree on the left, choose **Risk Prevention > Baseline Check**. On the baseline check page displayed, handle the baseline check items that fail the check.
- Step 5** In the navigation pane on the left, choose **Risk Prevention > Vulnerabilities**. On the vulnerability management page displayed, handle the vulnerabilities.
- Step 6** In the navigation pane on the left, choose **Threat Operations > Alert**. On the alert management page displayed, handle the alerts.
- Step 7** After the alert is handled, return to the **Security Overview** page and click **Check Again**. The security score will be updated then.

NOTE

It takes some time for a check to finish. You can refresh the page to get the new security score five minutes after you start the recheck.

----End

14.1.7 How Do I Handle a Brute-force Attack?

Brute-force attacks are common intrusion behavior. Attackers guess and try login usernames and passwords remotely. When they succeed, they can attack and control systems.

SecMaster works with HSS to receive alerts for brute force attacks detected by HSS and centrally display and manage alerts.

Handling Alerts

HSS uses brute-force detection algorithms and an IP address blacklist to effectively prevent brute-force attacks and block attacking IP addresses. Alerts will be reported.


If you receive an alert from HSS, log in to the HSS console to confirm and handle the alert.

- If your host is cracked and an intruder successfully logs in to the host, all hosts under your account may have been implanted with malicious programs. Take the following measures to handle the alert immediately to prevent further risks to the hosts:
 - a. Check whether the source IP address used to log in to the host is trusted immediately.
 - b. Change passwords of accounts involved.
 - c. Scan for risky accounts and handle suspicious accounts immediately.
 - d. Scan for malicious programs and remove them, if any, immediately.
- If your host is cracked and the attack source IP address is blocked by HSS, take the following measures to harden host security:
 - a. Check the source IP address used to log in to the host and ensure it is trusted.
 - b. Log in to the host and scan for OS risks.
 - c. Upgrade the HSS protection capability if it is possible.
 - d. Harden the host security group and firewall configurations based on site requirements.

Marking Alerts

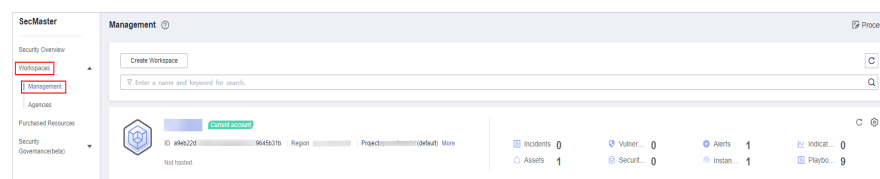
After an alert is handled, you can mark the alert.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Security > SecMaster**.

Step 3 In the navigation pane, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Figure 14-2 Management



Step 4 In the navigation pane on the left, choose **Threat Operations > Alert**. The alert management page is displayed.

Step 5 On the **Alert** tab, select **Brute-force attacks** and refresh the alert list.

Step 6 Delete the non-threat alerts.

----End

14.1.8 Why Is the Incident Data in SecMaster Inconsistent with That in WAF and HSS?

SecMaster aggregates all historical alert data reported by WAF and HSS, but WAF and HSS display real-time alert data. As a result, data in SecMaster is inconsistent with that in WAF and HSS.

Therefore, you are advised to go to the corresponding service (WAF or HSS) to view and handle the problem.

14.1.9 Troubleshooting the Agent Installation Failure

An agent needs to be installed on ECSs for security data collection. If the installation fails, you can fix the fault by following the instructions provided in this section.

Possible Causes

The possible causes are as follows:

- The network between the ECS where you want to install the Agent and the OBS bucket storing the Agent is disconnected.
- The disk space of the ECS server is insufficient.
- Failed to obtain the IAM token.
- Failed to verify the workspace ID.
- The Agent has been installed, while the system fails to find it.

Locating the Cause and Fixing the Failure

- The network between the ECS where you want to install the Agent and the OBS bucket storing the Agent is disconnected.

Figure 14-3 Disconnected network between the server and OBS

```

[root@host-192-168-0-10 ~]# wget https://csc-isp-logstash.obs.cn-north-1.amazonaws.com.cn/ispap-salt-obs/agent_controller_euler.sh 66
chmod +x agent_controller_euler.sh 66
./agent_controller_euler.sh install c18c4d92-2c3b54019 c148b0d0f6c [192.168.0.29,192.168.0.1]
2023-09-13 09:20:35 - https://csc-isp-logstash.obs.cn-north-1.amazonaws.com.cn/ispap-salt-obs/agent_controller_euler.sh
Resolving csc-isp-logstash.obs.cn-north-1.amazonaws.com (csc-isp-logstash.obs.cn-north-1.amazonaws.com)... failed: Name or service not known.
wget: unable to resolve host address 'csc-isp-logstash.obs.cn-north-1.amazonaws.com'
    
```

Solution

- (Optional) Method 1: Connect the ECS to OBS.
- (Optional) Method 2: Manually download the installation script and installation package to the local PC, and upload the installation package to the **/opt/cloud** directory on the server.
 - Log in to the OBS management console.
 - In the navigation pane on the left, choose **Buckets**. On the displayed page, click the name of the target bucket.

- iii. On the displayed details page, download the installation script and installation package.
- iv. Use a remote management tool, such as SecureFX or WinSCP, to log in to the server.
- v. Upload the installation package to the **/opt/cloud** directory on the server.
- **The disk space of the ECS is insufficient.**

Figure 14-4 Insufficient disk space



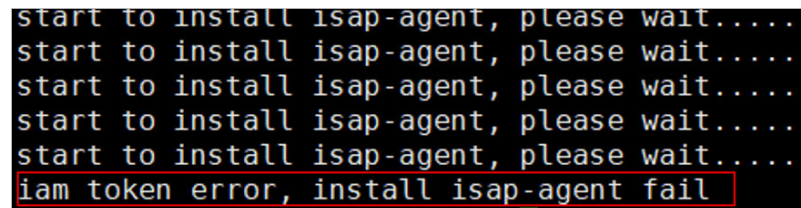
Solution

Clear the disk to reserve sufficient space.

- **Failed to obtain the IAM token.**
 - **Symptoms**

If information shown in the following figure is displayed in the log, the call to obtain IAM token failed.

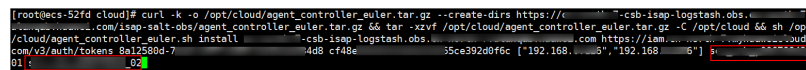
Figure 14-5 IAM token failure



- **Troubleshooting and Solution**

- i. Check whether the IAM account or username in the command is correct.

Figure 14-6 Username and password of an IAM user



- If any of them or both of them are incorrect, run the installation command with correct information again.
- If they are correct, go to **ii**.
- ii. Run the **vim /etc/salt/iam_token.txt** command to check whether the **/etc/salt/iam_token.txt** file exists.
 - If the information shown in the following figure is displayed, the directory exists. Go to **iii**.

- v. Check whether the workspace ID and project ID in the command are the same as those in the file in [iv](#).

Figure 14-11 Parameter information in the command

```
[root@ecs-...ud]# curl -k -o /opt/cloud/agent_controller_euler.tar.gz --create-dirs https://...csb-isap-logstash.obs...huawei.com/isap-salt-obs/agent_controller_euler.tar.gz && tar -zxvf /opt/cloud/agent_controller_euler.tar.gz -C /opt/cloud && chmod +x /opt/cloud/agent_controller_euler.sh && sh /opt/cloud/agent_controller_euler.sh install --workspaceid=f48e8...projectid=[*192.168...*,*192.168...*] sec_cs... 42.01
```

- vi. Use the correct workspace ID and project ID to run the command again.
- **The Agent has been installed, while the system fails to find it.**
 - **Symptoms**
If the information shown in the following figure is displayed, the Agent has been installed.

Figure 14-12 Agent installed already

```
warning: group servicegroup does not exist - using root
warning: user service does not exist - using root
warning: group servicegroup does not exist - using root
warning: user service does not exist - using root
warning: group servicegroup does not exist - using root
The ISAP-salt-minion-euler has been installed. Do not install the ISAP-salt-minion-euler again.
[root@ecs-...i]#
```

- **Solution**
 - i. (Optional) Method 1: Logging out the node on the management console.
 - 1) Log in to the SecMaster management console.
 - 2) In the navigation pane, choose **Workspaces**. In the workspace list, click the name of the target workspace.
 - 3) In the navigation tree on the left, choose **Settings > Component management**. On the node Management page, locate the row that contains the target node and click **Logout**.
 - 4) In the displayed dialog box, click **OK**.
 - ii. (Optional) Method 2: Run the script command to uninstall the Agent.
 - 1) Use a remote management tool, such as SecureFX or WinSCP, to log in to the server.
 - 2) Run the **sh /opt/cloud/agent_controller_euler.sh uninstall** command to uninstall the Agent.
 - iii. Check whether the uninstallation is complete.
 - 1) Use a remote management tool, such as SecureFX or WinSCP, to log in to the server.
 - 2) (Optional) Method 1: Run the **ls -a /opt/cloud/** command to view the files in the **/opt/cloud** directory. If the information shown in the following figure is displayed (including only the script file), the uninstallation is complete.

Figure 14-13 Script file

```
[root@ecs-...i]# ls -a /opt/cloud/
.. agent_controller_euler.sh
```

- 3) (Optional) Method 2: Run the **salt-minion --version** command. If the following information is displayed, the uninstallation is complete.

Figure 14-14 Checking Agent

```
[root@ecs-...]# salt-minion --version
-bash: salt-minion: command not found
```

 **CAUTION**

It takes some time to deregister a node. Do not install the Agent until you confirm that the node has been deregistered.

14.1.10 How Do I Grant Permissions to an IAM User?

If you want to authorize an IAM user to operate the SecMaster service, you need to use the primary account to grant permissions to the user.

Procedure

Step 1 Log in to the console as the administrator.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance > Identity and Access Management**.

Step 3 Create a user group.

1. In the navigation pane on the left, choose **User Groups**. On the displayed page, click **Create User Group** in the upper right corner.
2. On the **Create User Group** page, specify user group name and description.
 - **Name:** Set this parameter to **SecMaster_ops**.
 - **Description:** Enter a description.
3. Click **OK**.

Step 4 Create a custom policy.

1. In the navigation pane on the left, choose **Permissions > Policies/Roles**. In the upper right corner of the displayed page, click **Create Custom Policy**.
2. Configure a policy.
 - a. **Policy Name:** Set this parameter to **SecMaster_FullAccess**.
 - b. **Policy View:** Select **JSON**.
 - c. **Policy Content:** Copy the following content and paste it in the text box.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "secmaster:*:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

```
]
}
```

- a. Click **OK**.
- b. In the dialog box displayed, set the policy scope to **Global services**.
- c. Click **OK**.

Step 5 Assign permissions to the created user group.

1. In the navigation pane on the left, choose **User Groups**. On the displayed page, click **SecMaster_ops**.
2. On the **Permissions** tab page, click **Authorize**.
3. On the **Select Policy/Role** page, search for and select the **SecMaster_FullAccess** policy, and click **Next**.
4. Set the minimum authorization scope. Select **All resources** for **Scope**. After the setting is complete, click **OK**.

Step 6 Verify the authorization. The policy will be listed on the page.

----End

14.2 Purchase Consulting

14.2.1 How Do I Change SecMaster Editions or Specifications?

You can increase ECS quotas and buy a value-added package.

- Buy a value-added package: For details, see [Buying a Value-Add Pack](#).
- Increase ECS quotas: For details, see [Increasing the Quota](#).

14.2.2 How Is SecMaster Billed?

SecMaster is billed in pay-per-use mode. In this mode, you are billed for usage duration by the hour. This mode allows you to enable or disable the SecMaster service at any time.

14.2.3 Can I Unsubscribe from SecMaster?

If you no longer need SecMaster, unsubscribe from it or cancel it in just a few clicks.

- Pay-per-use billing mode: pay for what you use by the hour. This mode allows you to enable or disable resources at any time. One-click resource cancellation is also supported.

Limitations and Constraints

- In the **pay-per-use** professional edition, when you unsubscribe from or cancel the asset quota of the professional edition, the plus package is also unsubscribed or canceled.

Canceling Pay-per-Use SecMaster Resources

- Step 1** Click **Professional** in the upper right corner. The edition management window is displayed.
- Step 2** In the row of the SecMaster edition purchased in pay-per-use billing mode, click **Cancel** to release the purchased SecMaster resources.

Go to the edition management window and verify that the subscription to resources billed on a pay-per-use basis is canceled.

----End

Unsubscribing from a Plus Features

- Step 1** Click **Professional** in the upper right corner. A window for you to manage SecMaster assets will be displayed.
- Step 2** Click **Cancel** to release the pay-per-use asset quota. Go to the edition management window and verify that the pay-per-use asset quota is canceled.

----End

A Change History

Released On	Description
2023-09-20	<p>This issue is the second official release.</p> <ul style="list-style-type: none"> • Optimized GUI description of "Overall Situation", "Asset Security", and "Threat Situation" under Large Screen and updated section "Viewing Vulnerable Asset Information." • Updated procedure and optimized parameter description in sections "Repairing Vulnerabilities", "Managing Vulnerabilities", "Adding Intelligence Indicators", "Managing Models", "Creating a Data Delivery", and "Managing Components." • Optimized the procedure in sections "Viewing Alert Information" and "Disabling or Deleting Alerts." • Updated the screenshots for available models in section "Creating/Editing a Model."
2023-07-31	This issue is the first official release.