

SecMaster

User Guide

Issue 03
Date 2024-10-30



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

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

Trademarks and Permissions



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

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

Notice

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

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

Contents

1 Service Overview.....	1
1.1 What Is SecMaster?.....	1
1.2 What Is a SOC?.....	1
1.3 Product Advantages.....	8
1.4 Application Scenarios.....	8
1.5 Functions.....	9
1.6 SecMaster and Other Services.....	15
1.7 Basic Concepts.....	15
2 Authorizing SecMaster.....	18
3 Security Overview.....	19
3.1 Overview.....	19
3.2 Security Score.....	23
4 Workspaces.....	26
4.1 Workspace Overview.....	26
4.2 Creating a Workspace.....	26
4.3 Managing Workspaces.....	27
4.3.1 Viewing Workspace Details.....	28
4.3.2 Editing a Workspace.....	29
4.3.3 Managing Workspace Tags.....	29
4.3.4 Deleting a Workspace.....	30
5 Viewing Purchased Resources.....	32
6 Security Situation.....	33
6.1 Situation Overview.....	33
6.2 Large Screen.....	40
6.2.1 Overall Situation Screen.....	40
6.2.2 Security Response Screen.....	46
6.2.3 Asset Security Screen.....	50
6.2.4 Threat Situation Screen.....	53
6.2.5 Vulnerability Situation Screen.....	57
6.3 Security Reports.....	60
6.3.1 Creating and Copying a Security Report.....	60

6.3.2 Viewing a Security Report.....	63
6.3.3 Downloading a Security Report.....	72
6.3.4 Managing Security Reports.....	73
6.4 Task Center.....	74
6.4.1 Viewing To-Do Tasks.....	74
6.4.2 Handling a To-Do Task.....	75
6.4.3 Viewing Completed Tasks.....	76
7 Resource Manager.....	78
7.1 Overview.....	78
7.2 Configuring the Asset Subscription.....	78
7.3 Viewing Resource Information.....	79
7.4 Importing and Exporting Assets.....	80
7.5 Editing and Deleting Resources.....	82
8 Risk Prevention.....	84
8.1 Baseline Inspection.....	84
8.1.1 Baseline Inspection Overview.....	84
8.1.2 Creating a Custom Check Plan.....	85
8.1.3 Starting an Immediate Baseline Check.....	87
8.1.4 Viewing Check Results.....	89
8.1.5 Handling Check Results.....	91
8.1.6 Viewing Compliance Packs.....	94
8.1.7 Creating a Custom Compliance Pack.....	95
8.1.8 Importing and Exporting a Compliance Pack.....	97
8.1.9 Viewing Check Items.....	98
8.1.10 Creating a Custom Check Item.....	99
8.1.11 Importing and Exporting Check Items.....	101
8.2 Vulnerability Management.....	102
8.2.1 Overview.....	102
8.2.2 Viewing Vulnerability Details.....	103
8.2.3 Fixing Vulnerabilities.....	105
8.2.4 Importing and Exporting Vulnerabilities.....	107
8.2.5 Ignoring and Unignoring a Vulnerability.....	109
8.3 Policy Management.....	110
8.3.1 Overview.....	110
8.3.2 Adding and Editing an Emergency Policy.....	110
8.3.3 Viewing Emergency Policies.....	113
8.3.4 Deleting an Emergency Policy.....	114
8.3.5 Blocking or Canceling Blocking of an IP Address or IP Address Range.....	115
9 Threat Operations.....	117
9.1 Incident Management.....	117
9.1.1 Viewing Incidents.....	117

9.1.2 Adding and Editing an Incident.....	119
9.1.3 Importing and Exporting Incidents.....	123
9.1.4 Closing or Deleting Incidents.....	124
9.2 Alert Management.....	125
9.2.1 Viewing Alerts.....	125
9.2.2 Converting an Alert to an Incident or Associating an Alert with an Incident.....	127
9.2.3 Adding and Editing an Alert.....	135
9.2.4 Importing and Exporting Alerts.....	138
9.2.5 Closing or Deleting an Alert.....	139
9.2.6 One-click Blocking or Unblocking.....	140
9.3 Indicator Management.....	142
9.3.1 Adding and Editing an Indicator.....	142
9.3.2 Disabling and Deleting an Indicator.....	145
9.3.3 Importing and Exporting Intelligence Indicators.....	145
9.3.4 Viewing Indicators.....	147
9.4 Intelligent Modeling.....	148
9.4.1 Viewing Available Model Templates.....	148
9.4.2 Creating and Editing a Model.....	149
9.4.3 Viewing Available Models.....	156
9.4.4 Managing Models.....	157
9.5 Security Analysis.....	158
9.5.1 Security Analysis Overview.....	158
9.5.2 How to Use Security Analysis.....	158
9.5.3 Log Fields.....	159
9.5.4 Configuring Indexes.....	203
9.5.5 Querying and Analyzing Data.....	205
9.5.6 Downloading Logs.....	208
9.5.7 Query and Analysis Statements - SQL Syntax.....	208
9.5.7.1 Basic Syntax.....	209
9.5.7.2 Limitations and Constraints.....	209
9.5.7.3 Query Statements.....	209
9.5.7.4 Analysis Statements - SELECT.....	211
9.5.7.5 Analysis Statements - GROUP BY.....	213
9.5.7.6 Analysis Statements - HAVING.....	214
9.5.7.7 Analysis Statements - ORDER BY.....	215
9.5.7.8 Analysis Statements - LIMIT.....	215
9.5.7.9 Analysis Statements - Functions.....	216
9.5.7.10 Analysis Statements - Aggregate Functions.....	221
9.5.8 Quick Query.....	222
9.5.9 Quickly Adding a Log Alarm Model.....	223
9.5.10 Charts.....	226
9.5.10.1 Overview.....	226

9.5.10.2 Tables.....	226
9.5.10.3 Line Charts.....	227
9.5.10.4 Bar Charts.....	228
9.5.10.5 Pie Charts.....	230
9.5.11 Managing Data Spaces.....	231
9.5.11.1 Creating a Data Space.....	231
9.5.11.2 Viewing Data Space Details.....	232
9.5.11.3 Editing a Data Space.....	233
9.5.11.4 Deleting a Data Space.....	234
9.5.12 Managing Pipelines.....	234
9.5.12.1 Creating a Pipeline.....	235
9.5.12.2 Viewing Pipeline Details.....	236
9.5.12.3 Editing a Pipeline.....	237
9.5.12.4 Deleting a Pipeline.....	238
9.5.13 Data Consumption.....	239
9.5.14 Data Monitoring.....	240
9.6 Data Delivery.....	241
9.6.1 Creating a Data Delivery.....	241
9.6.2 Data Delivery Authorization.....	244
9.6.3 Checking the Data Delivery Status.....	246
9.6.4 Managing Data Delivery.....	247
9.6.5 Delivering Logs to LTS.....	249
10 Security Orchestration.....	252
10.1 Security Orchestration Overview.....	252
10.2 Built-in Playbooks.....	253
10.3 Security Orchestration Process.....	256
10.4 (Optional) Configuring and Enabling a Workflow.....	258
10.5 Configuring and Enabling a Playbook.....	261
10.6 Operation Object Management.....	262
10.6.1 Data Class.....	262
10.6.1.1 Viewing Data Classes.....	262
10.6.2 Type Management.....	263
10.6.2.1 Managing Alert Types.....	263
10.6.2.2 Managing Incident Types.....	268
10.6.2.3 Managing Threat Intelligence Types.....	272
10.6.2.4 Managing Vulnerability Types.....	277
10.6.2.5 Managing Custom Types.....	281
10.6.3 Classification & Mapping.....	287
10.6.3.1 Viewing Categorical Mappings.....	287
10.6.3.2 Creating, Copying, and Editing a Categorical Mapping.....	288
10.6.3.3 Managing Categorical Mappings.....	290
10.7 Playbook Orchestration Management.....	291

10.7.1 Playbooks.....	291
10.7.1.1 Submitting a Playbook Version.....	292
10.7.1.2 Reviewing a Playbook Version.....	292
10.7.1.3 Enabling a Playbook.....	294
10.7.1.4 Managing Playbooks.....	294
10.7.1.5 Managing Playbook Versions.....	297
10.7.2 Workflows.....	299
10.7.2.1 Reviewing a Workflow Version.....	299
10.7.2.2 Enabling a Workflow.....	300
10.7.2.3 Managing Workflows.....	301
10.7.2.4 Managing Workflow Versions.....	304
10.7.3 Asset Connections.....	308
10.7.3.1 Adding an Asset Connection.....	308
10.7.3.2 Managing Asset Connections.....	310
10.7.4 Instance Management.....	312
10.7.4.1 Viewing Monitored Playbook Instances.....	312
10.8 Layout Management.....	314
10.8.1 Viewing an Existing Layout Template.....	314
10.8.2 Manage Existing Layouts.....	315
10.9 Plug-in Management.....	316
10.9.1 Plug-in Management Overview.....	316
10.9.2 Viewing Plug-in Details.....	316
11 Settings.....	318
11.1 Data Collection.....	318
11.1.1 Data Collection Overview.....	318
11.1.2 Component Management.....	323
11.1.2.1 Creating and Editing a Node.....	323
11.1.2.2 Partitioning a Disk.....	326
11.1.2.3 Managing Nodes.....	328
11.1.2.4 Configuring a Component.....	329
11.1.2.5 Logstash Configuration Description.....	330
11.1.2.6 Viewing Component Details.....	332
11.1.3 Collection Management.....	333
11.1.3.1 Adding and Editing a Connection.....	333
11.1.3.2 Rules for Configuring Connectors.....	334
11.1.3.3 Managing Connections.....	348
11.1.3.4 Creating and Editing a Parser.....	349
11.1.3.5 Rules for Configuring Parsers.....	352
11.1.3.6 Managing Parsers.....	359
11.1.3.7 Adding and Editing a Collection Channel.....	361
11.1.3.8 Managing Collection Channels.....	366
11.1.3.9 Viewing Collection Nodes.....	367

11.1.4 Upgrading the Component Controller.....	368
11.2 Data Integration.....	370
11.2.1 Log Access Supported by SecMaster.....	370
11.2.2 Enabling Log Access.....	370
11.3 Customizing Directories.....	372
12 FAQs.....	374
12.1 Product Consulting.....	374
12.1.1 Why Is There No Attack Data or Only A Small Amount of Attack Data?.....	374
12.1.2 Where Does SecMaster Obtain Its Data From?.....	374
12.1.3 What Are the Dependencies and Differences Between SecMaster and Other Security Services?...	375
12.1.4 What Are the Differences Between SecMaster and HSS?.....	376
12.1.5 How Do I Update My Security Score?.....	378
12.1.6 How Do I Handle a Brute-force Attack?.....	378
12.1.7 Issues About Data Synchronization and Data Consistency.....	379
12.2 About Data Collection Faults.....	380
12.2.1 Component Controller Installation Failure.....	380
12.2.2 Collection Node or Collection Channel Faults.....	383
12.2.3 Common Commands for the Component Controller.....	387
A Change History.....	388

1 Service Overview

1.1 What Is SecMaster?

SecMaster is a next-generation cloud native **security operations center**. 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.

Why SecMaster?

- Comprehensive awareness on one screen: Alert incidents of security services are collected, associated, sorted, and made available for retrieval, enabling security operation situations to be comprehensively evaluated and dynamically displayed on a large screen.
- Global analysis on one cloud: SecMaster locates threats based on hundreds of millions of threat indicators every day, eliminates invalid alerts, and identifies potential advanced threats.
- Integrated global handling: The built-in alert processing playbooks enable minute-level automatic response to more than 99% security incidents.

1.2 What Is a SOC?

A security operations center (SOC) is a centralized function or team that checks all activities on endpoints, servers, databases, network applications, websites, and other systems around the clock to detect potential threats in real time. It aims to improve enterprise cybersecurity posture by prevention, analysis, and responses of cybersecurity events. A SOC also obtains latest threat intelligence to keep up-to-date information about threat groups and infrastructure. As a proactive defense system, a SOC always identifies and handles vulnerabilities in services systems or processes before attackers exploit them. Most SOCs run around the clock, seven days a week. Some cross-countries/regions enterprises or organizations may also rely on Global Security Operations Centers (GSOs) to learn of global security threats and coordinate detection and response across local SOCs.

What a SOC Does

A SOC team has the following responsibilities to help prevent, respond to, and recover services from attacks.

- **Asset and tool inventory**

To eliminate blind spots in protection, a SOC needs to know every asset that needs to be protected and all tools used to protect them in the organization. This means a SOC needs to cover all databases, cloud services, identities, applications, and clients across on-premises data centers and clouds. A SOC also needs to know all security solutions used in the organization, for example, firewalls, anti-malware, anti-ransomware, and monitoring software.

- **Reducing attack surface**

A key responsibility of a SOC is to reduce the attack surface of the organization. To do this, SOC needs to maintain an exhaustive inventory of all workloads and assets, apply security patches to software and firewalls, identify misconfigurations, and discover and add new assets as they come online. SOC team members are also responsible for researching emerging threats and analyzing risks. This helps the SOC keep ahead of the latest threats.

- **Continuous monitoring**

A SOC team uses a security analysis solution to monitor the entire environment, covering on-premises, cloud, applications, networks, and devices, all day to detect abnormal or suspicious behavior. The solution can be a security information enterprise management (SIEM), security orchestration, automation, and response (SOAR), and extended detection and response (XDR) solution. These tools collect telemetry data, aggregate the data, and, in some cases, automate incident responses.

- **Threat intelligence**

A SOC also uses data analysis, external sources, and product threat reports to gain an in-depth insight into attacker behavior, infrastructure, and motives. This intelligence provides a comprehensive view of what is happening across the Internet and helps the team understand how groups work. With this information, the SOC can quickly detect threats and enhance the responses to emerging risks.

- **Threat detection**

SOC teams use the data generated by the SIEM and XDR solutions to identify threats. This first step is to filter out false positives from real issues. They then prioritize threats by severity and potential impact on services.

- **Log management**

A SOC also collects, maintains, and analyzes log data generated by each client, operating system, VM, local application, and network incident. SOC's analysis helps establish a baseline for normal activity and reveals anomalies that may indicate malware, ransomware, or viruses.

- **Incident response**

Once an online attack is identified, the SOC quickly takes actions to limit the damage to the organization with as little impacts on services as possible. Those actions may include shutting down or isolating affected clients and applications, suspending compromised accounts, removing infected files, and running anti-virus and anti-malware software.

- **Recovery and remediation**

After an attack, a SOC is responsible for restoring organization's services to its original state. The team will erase and reconnect the disk, identity, email, and clients, restart the application, switch to the backup system, and restore data.
- **Root cause investigation**

To prevent similar attacks from happening again, the SOC conducts a thorough investigation to identify vulnerabilities, ineffective security processes, and other experiences that led to the incident.
- **Security refinement**

A SOC uses any intelligence gathered during an incident to fix vulnerabilities, improve processes and policies, and update the security roadmap.
- **Compliance management**

A key part of a SOC's responsibility is to ensure that applications, security tools, and processes comply with privacy regulations, such as *PCI DSS Security Compliance Package*, *ISO 27701 Security Compliance Package*, and *ISO 27001 Security Compliance Package*. The team regularly reviews the system to ensure compliance and to make sure that regulators, law enforcement, and customers are notified of data breaches.

Key Roles in a SOC

Based on the scale of an organization, a typical SOC includes the following roles:

- **Incident response director**

This role, which is typically planned in very large organizations, is responsible for coordinating detection, analysis, containment, and recovery during a security incident. They also manage communication with corresponding stakeholders.
- **SOC manager**

A SOC manager oversees the SOC. They are responsible for reporting to the Chief Information Security Officer (CISO). Their responsibilities include supervising personnel, running services, training new employees and managing finance.
- **Security engineer**

Security engineers are responsible for operating of the organization's security system. This includes designing security architectures and researching, implementing, and maintaining security solutions.
- **Security analyst**

A security analyst is the first responder in a security incident. They are responsible for identifying threats, prioritizing threats, and then taking actions to contain damage. During an online attack, they may need to isolate infected hosts, clients, or users. In some organizations, security analysts are graded based on the security severity of the threats they are responsible for addressing.
- **Threat hunter**

In some organizations, the most experienced security analysts are called threat hunters. They identify and respond to advanced threats that are not detected by automated tools. This role is proactive and designed to deepen

the organization's understanding of known threats and reveal unknown threats before attacks actually occur.

- **Forensics analyst**

Large organizations may also hire forensic analysts who are responsible for collecting intelligence to determine the root causes of violations. They search for system vulnerabilities, violations against security policies, and cyber attack patterns that may be useful in preventing similar intrusions in the future.

Types of SOCs

There are several ways for organizations to set up their SOCs. Some organizations choose to build dedicated SOCs with full-time employees. This type of SOC can be internal, with a physical local location, or can be virtual, with employees coordinating their work remotely using digital tools. Many virtual SOCs have both contract workers and full-time employees. An outsourced SOC, also called "managed SOC" or "SOC as a service", is run by a managed security service provider who is responsible for preventing, detecting, investigating, and responding to threats. An organization may also use a combination of internal employees and a managed security service provider. This way is called a co-managed or hybrid SOC. Organizations use this approach to increase the influence of their employees. For example, if they do not have threat investigators, it may be easier to hire third parties than to equip them internally.

Importance of a SOC Team

A strong SOC can help enterprises, governments, and other organizations stay ahead of an evolving online threat landscape. It is not an easy task. Both attacks and defense communities often develop new technologies and strategies, and it takes time and efforts to manage all changes. A SOC can leverage its understanding of the broader cybersecurity environment and of internal weaknesses and service priorities to help organizations develop a security roadmap that meets long-term business needs. SOCs can also limit the impact of attacks on services. Since they are continuously monitoring the network and analyzing alert data, they are more likely to detect threats earlier than other teams scattered among other priorities. Through regular training and well-documented processes, SOCs can quickly handle current incidents, even under great pressure. This can be difficult for teams that do not have a round-the-clock focus on secure operations.

Benefits of a SOC

By unifying the personnel, tools, and processes to protect an organization from threats, a SOC helps the organization defend against attacks and breaches more effectively and efficiently.

- **Strong security situation**

Improving the security of an organization is a job that has no ends. It requires continuous monitoring, analysis, and planning to discover vulnerabilities and master changing technologies. If several tasks have the same priority, it is more likely to ignore security and focus on tasks that seem more urgent.

A centralized SOC helps make sure that processes and technologies are improved continuously, reducing the risk of successful attacks.

- **Compliance with privacy laws and regulations**

In different industries, countries, and regions, there are many regulations that govern the collection, storage, and use of data. Many regulations require organizations to report data breaches and detect personal data upon user requests. Developing appropriate processes and procedures is as important as having the right technology. SOC members help organizations comply with these regulations by taking responsibility for keeping technology and data processes up to date.

- **Swift incident responses**

How quickly cyber attacks can be detected and prevented is critical. With appropriate tools, personnel, and intelligence, vulnerabilities can be curbed before they cause any damage. But bad actors are also smart, they may hide in the system to steal massive amount of data and escalate their permissions before anyone notices. A security incident is also a very stressful thing, especially for those who lack experience in incident response.

With unified threat intelligence and well-documented procedures, a SOC team can quickly detect, respond to, and recover from attacks.

- **Reduced breach costs**

A successful intrusion can be very expensive for organizations. It may lead to a long downtime before service recovery. Some organizations may lose customers or find it difficult to win new customers shortly after an incident. By acting ahead of attackers and responding quickly, a SOC helps organizations save time and money when they return to normal operations.

Best Practices for SOC Teams

With so many things to be responsible for, a SOC must effectively manage to achieve expected results. Organizations with strong SOCs implement the following security practices:

- **Service-aligned strategy**

Even the most well-funded SOC has to decide where to spend its time and money. Organizations usually conduct risk assessments first to identify the aspects that are most vulnerable to risks and the greatest business opportunities. This helps to determine what needs to be protected. A SOC also needs to know the environment where the assets are located. Many enterprises have complex environments, with some data and applications on-premises and some distributed across clouds. A strategy helps determine whether security professionals need to be available at all hours every day and whether it is better to set up an in-house SOC or to use professional services.

- **Talented, well-trained employees**

The key to an effective SOC lies in highly skilled and progressive employees. The first step is to find the best talent. However, this can be tricky as the market for security personnel is really competitive. To avoid skill gaps, many organizations try to find people with a variety of expertise, including systems and intelligence monitoring, alert management, incident detection and analysis, threat hunting, ethical hacking, cyber forensics, and reverse engineering. They also deploy technologies that automate tasks to make smaller teams more efficient and improve the output of junior analysts. Investing in regular training helps organizations keep key employees, fill skills gaps, and develop employees' careers.

- **End-to-end visibility**
An attack may start with a single client, so it is critical for the SOC to understand the entire environment of the organization, including anything managed by a third party.
- **Right tools**
There are so many security incidents that teams can be easily overwhelmed. Effective SOCs invest in excellent security tools that work well together and use AI and automation to report major risks. Interoperability is the key to avoiding coverage gaps.

SOC Tools and Technologies

- **Security information and event management (SIEM)**
One of the most important tools in a SOC is a cloud-based SIEM solution, which aggregates data from multiple security solutions and log files. With threat intelligence and AI, these tools help SOCs detect evolving threats, accelerate incident response, and act before attackers.
- **Security orchestration, automation and response (SOAR)**
A SOAR automates periodic and predictable actions, response, and remediation tasks, freeing up time and resources for more in-depth investigations and hunting.
- **Extended detection and response (XDR)**
XDR is a service-oriented software tool that provides comprehensive and better security by integrating security products and data into simplified solutions. Organizations use these solutions to proactively and effectively address an evolving threat landscape and complex security challenges across clouds. Compared with systems such as endpoint detection and response (EDR), XDR expands the security scope to integrate protection across a wider range of products, including organization's endpoints, servers, cloud applications, and emails. On this basis, XDR combines prevention, detection, investigation, and response to provide visibility, analysis, correlated incident alerts, and automated response to enhance data security and combat threats.
- **Firewall**
A firewall monitors incoming and outgoing network traffic and allows or blocks the traffic based on the security rules defined by the SOC.
- **Log management**
A log management solution is usually part of a SIEM. It logs all alerts from each software, hardware, and client running in the organization. These logs provide information about network activities.
- **Vulnerability management**
Vulnerability management tools scan the network to help identify any weaknesses that attackers may exploit.
- **User and entity behavior analytics (UEBA)**
User and entity behavior analytics (UEBA) is built in many modern security tools. UEBA uses AI to analyze data collected from varied devices to establish a baseline of normal activity for each user and entity. When an event deviates from the baseline, it will be marked for further analysis.

SOC and SIEM

Without a SIEM, a SOC will be difficult to accomplish its tasks. Today's SIEM provides the following functions:

- Log aggregation: A SIEM collects log data and associates alerts. Analysts can use the information to detect and search for threats.
- Context: SIEM collects data across all technologies in the organization, so it helps connect points between individual incidents and identify sophisticated attacks.
- Alert reduction: A SIEM uses analytics and AI to correlate alerts and identify the most serious incidents, reducing the number of false positives.
- Automatic response: A SIEM uses built-in rules to identify and prevent possible threats without human interaction.

NOTE

It is also important to note that a SIEM alone is not enough to protect the organization. Users need to integrate a SIEM with other systems, define parameters for rule-based detection, and evaluate alerts. So it is critical to define the SOC strategy and hire the appropriate staff.

SOC Solution

There are multiple solutions that can be used to help a SOC protect the organization. The best solution works together with other security services to provide complete coverage across on-premises and multiple clouds. Our company provides a comprehensive solution to help SOC narrow the gap in protection coverage and give a 360-degree view of your environment. SecMaster integrates the detection and response solution to provide analysts and threat hunters with the data they need to find and contain cyber attacks.

FAQs

1. What does a SOC team need to do?
A SOC team monitors servers, devices, databases, network applications, websites, and other systems to detect potential threats in real time. The team performs proactive security efforts. They keep abreast of the latest threats and discover and resolve system or process vulnerabilities before attackers exploit them. If an organization is being attacked, the SOC team is responsible for eradicating the threat and restoring the system and backup as needed.
2. What are the key components in a SOC?
A SOC consists of people, tools, and processes that help protect the organization from cyber attacks. To achieve its objectives, an SOC performs the following functions: inventory of all assets and security techniques, routine maintenance and preparation, continuous monitoring, threat detection, threat intelligence, log management, incident response, recovery and remediation, root cause investigation, security optimization, and compliance management.
3. Why do organizations need strong SOC?
A strong SOC helps organizations manage security more efficiently and effectively through unified defense, threat detection tools, and security processes. Organizations with SOC can improve their security processes,

respond to threats faster, and better manage compliance than those without SOCs.

4. What are the differences between a SIEM and a SOC?

A SOC consists of the personnel, processes, and tools responsible for protecting organizations from cyber attacks. A SIEM is one of the many tools used by a SOC to maintain visibility and respond to attacks. A SIEM aggregates logs and uses analytics and automation to reveal credible threats to SOC members who decide how to respond.

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. By analyzing billions of security logs daily and leveraging the years of experience accumulated, SecMaster utilizes built-in models and analysis playbooks to reduce the interference from 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 Functions

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

This topic introduces SecMaster editions and their function differences.

Security Overview

The Security Overview page gives you a comprehensive view of your asset security posture together with other linked cloud security services to centrally display security assessment findings.

Table 1-1 Functions

Function Module	Description
Security Overview	<ul style="list-style-type: none"> Security Score: A 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. The lower the security score, the greater the overall asset security risk. Security Monitoring: You can view how many threats, vulnerabilities, and compliance violations that are not handled and view their details. Security Scores over the Time: You can view the trend of the asset health scores for the last seven 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	<ul style="list-style-type: none"> Workspace management: Workspaces are top-level workbenches in SecMaster. A single workspace can be bound to projects and regions to support workspace operational modes in different scenarios.

Purchased Resources

Purchased Resources centrally displays the resources purchased by the current account, making it easier for you to manage them in one place.

Table 1-3 Functions

Function Module	Description
Purchased Resources	You can view resources purchased by the current account on the Purchased Resources page and manage them centrally.

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 1-4 Functions

Function Module	Description
Situation Overview	<ul style="list-style-type: none"> • Security Score: A 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. The lower the security score, the greater the overall asset security risk. • Security Monitoring: You can view how many threats, vulnerabilities, and compliance violations that are not handled and view their details. • Security Scores over the Time: You can view the trend of the asset health scores for the last seven days.
Large Screen	<p>SecMaster leverages AI to analyze and classify massive cloud security data and then displays real-time results on a large screen. In a simple, intuitive, and efficient way, you will learn of what risks your cloud environment are facing and how secure your cloud environment is.</p> <p>NOTE The large screen function needs to be applied for separately.</p>
Security Reports	You can generate analysis reports and periodically send them to specified recipients by email. In this way, all recipients can learn about the security status of your assets in a timely manner.
Task Center	All tasks that need to be processed are displayed centrally.

Resource Manager

Resource Manager supports centralized management of assets on the cloud and assets outside the cloud and displays their security status in real time.

Table 1-5 Functions

Function Module	Description	Basic	Standard	Professional
Resource Manager	SecMaster can synchronize the security statistics of all resources. So that you can check the name, service, and security status of a resource to quickly locate security risks.	×	√	√

Table 1-6 Functions

Function Module	Description
Resource Manager	SecMaster can synchronize the security statistics of all resources. So that you can check the name, service, and security status of a resource to quickly locate security risks.

Risk Prevention

Risk prevention provides baseline check and vulnerability management functions to help you check cloud security configurations in accordance with many security standards. You will know where vulnerabilities are located in the entire environment.

Table 1-7 Functions

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	SecMaster automatically synchronizes vulnerability scan result from Host Security Service (HSS), displays vulnerability scan details by category, and provides vulnerability fixing suggestions.
Security Policies	SecMaster supports centralized management of defense and emergency policies.

Threat Operations

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 1-8 Functions

Function Module	Description
Incidents	SecMaster centrally displays incident details and allows you to manually or automatically convert alerts into incidents.

Function Module	Description
Alerts	This module provides unified data class (security operations objects) management and built-in alert reporting standards. Alerts of other cloud services such as HSS, WAF, and DDoS Mitigation are integrated and centrally displayed.
Indicators	This module provides unified data class (security operation objects) management and built-in threat intelligence indicator library. Security indicators from other cloud services can be accessed, and custom rules for extracting indicators are supported.
Intelligent Modeling	Models are supported to scan log data in pipelines. If SecMaster detects data that hits the trigger in a model, SecMaster generates an alert.
Security Analysis	<ul style="list-style-type: none"> • 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: Data analysis is visualized to intuitively reflect service structure and trend, so that you can create custom analysis reports and analysis indicators easily. • Data delivery: SecMaster can deliver data to other pipelines or other cloud products in real time so that you can store data or consume data with other systems. • Data monitoring: SecMaster supports end-to-end data traffic monitoring and management. • Data consumption: SecMaster provides streaming communication interfaces for data consumption and production and data pipelines that are integrated in SDKs. You can use SDKs to integrate data across systems and customize data consumers and producers. SecMaster provides open-source log collection plug-in Logstash. You can enable custom data consumers and producers. <p>NOTE You need to apply for the security analysis function separately.</p>

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 1-9 Functions

Function Module	Description
Objects	This module helps centrally manage operation objects such as data classes, data class types, and categorical mappings.
Playbooks	This module supports full lifecycle management of playbooks, workflows, asset connections, and instances.
Layouts	This module provides a visualized low-code development platform. In this module, you can create custom layout of pages for security analysis reports, alert management, incident management, vulnerability management, baseline management, and threat indicator library management. NOTE You need to separately apply for the security orchestration function in the value-added package.
Plugins	Plug-ins used in the security orchestration process can be managed centrally.

Data Collection

Collects varied 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 1-10 Functions

Function Module	Description
Data Collection (Collections and Components)	Logstash is used to collect varied 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

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

Table 1-11 Functions

Function Module	Description
Data Integration	SecMaster provides a preset log collection system. You can enable access to logs of other cloud services in just a few clicks. You can search and analyze all collected logs in SecMaster.

Directory Customization

You can customize directories as needed.

Table 1-12 Functions

Function Module	Description
Directory Customization	You can view in-use directories and change their layouts.

1.6 SecMaster and Other Services

This topic describes SecMaster and its linked services.

Security Services

SecMaster aggregates security event records from other 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.

1.7 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 common 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


Scenario

SecMaster depends on some other cloud services. To better use SecMaster, you can authorize SecMaster to perform some operations on some cloud services on your behalf. For example, you can allow SecMaster to execute scheduling tasks and manage resources.

Your authorization is required first time you try to use SecMaster.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 (Optional) In the upper part of the workspace management page, click **Entrusted Service Authorization - Current Tenant**.

The service authorization page is automatically displayed the first time you log in.

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 Security Overview

3.1 Overview

On the **Security Overview** page, SecMaster displays the overall security assessment result of your assets in real time. SecMaster works together with other cloud security services to centrally display security assessment and monitoring results, as well as your cloud security scores over time.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper part 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](#)

The following table describes the reference periods and update frequency of the modules.

Table 3-1 Security Overview

Parameter	Statistical Period	Update Frequency	Description
Security Score	Real-time	<ul style="list-style-type: none"> Automatic update at 02:00 every day Updated every time you click Check Again 	The score is calculated based on what security services are enabled, and the levels and numbers of unhandled configuration issues, vulnerabilities, and threats. For details, see Security Score .
Threat Alarms	Last 7 days	Every 5 minutes	Total number of alerts in all SecMaster workspaces of your account.
Vulnerabilities	Last 7 days	Every 5 minutes	Total number of vulnerabilities in all SecMaster workspaces of your account.
Abnormal Baseline Settings	Real-time	Every 5 minutes	Total number of abnormal baseline settings in all SecMaster workspaces of your account.
Your Security Score over Time	Last 7 days	Every 5 minutes	Security scores in the last seven days.

----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.

- The security score is automatically updated at 02:00 every day. You can also click **Check Again** to update it immediately.
- 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.

Table 3-2 Security Monitoring parameters

Parameter	Description
Threat Alarms	<p>This panel displays the unhandled threat alerts in all workspace of the current account 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. The statistics are updated every 5 minutes.</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 in all workspaces of your account 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. The statistics are updated every 5 minutes.</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 the five vulnerability types with the most affected servers. <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 compliance violations detected in all workspaces of your account. You can quickly learn of total number of violations and the number of violations at each severity level. The statistics are updated every 5 minutes.</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, 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.

Your Security Score over Time

SecMaster displays your security scores over the **last 7 days**. The statistics are updated every 5 minutes.

3.2 Security Score

Scenario

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

The security score is automatically updated at 02:00 every day. You can also click **Check Again** to update it immediately.

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 six 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**.
- If you have fixed asset risks and refreshed the alert status, you can click **Check Again** to update the security score.

 **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 3-3 Security score table

Severity	Security Score	Description
Secure	100	Congratulations. Your assets are secure.
Informat ional	$80 \leq \text{Security Score} < 100$	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 3-4 lists the security check items and corresponding points.

Table 3-4 Unscored check items

Category	Unscored Item	Unsocred Point	Suggestion	Maximum Unscored Point
Enabling of security services	Security-related services not enabled	-	Enable security-related services.	30

Category	Unscored Item	Unscored Point	Suggestion	Maximum Unscored Point
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		

4 Workspaces

4.1 Workspace Overview

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

What Is a Workspace?

A workspace is the top-level operation platform in SecMaster.

- **Workspace management:**
A single workspace can be bound to common projects to support workspace operation modes in different 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.

4.2 Creating a Workspace

Scenario

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

Before using baseline inspection, alert management, security analysis, and security orchestration in SecMaster, you need to create at least one workspace first. You can use workspaces to group your resources by application scenario. This will make security operations more efficient.

This section describes how to create a workspace.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**.
- Step 4** On the **Management** page, click **Create**. The **Create Workspace** slide-out panel is displayed.
- Step 5** Configure workspace parameters by referring to the following table.

Table 4-1 Creating a workspace

Parameter	Description
Region	Select the region where you want to add the workspace.
Enterprise Project	Select an enterprise project from the drop-down list. This option is only available when you are logged in using an enterprise account, or when 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 displayed 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

4.3 Managing Workspaces


4.3.1 Viewing Workspace Details

Scenario

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

Procedure

Step 1 Log in to the management console.

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

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

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

If there are many workspaces, you can use filters to quickly search for a specific workspace.

Figure 4-1 Workspace details

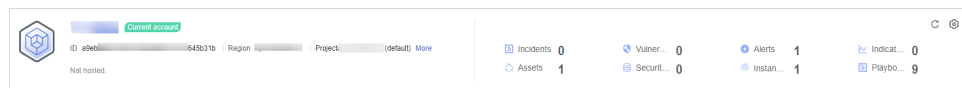



Table 4-2 Workspace parameters

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	Move the pointer over More to view the 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.

On the **Basic Information** tab, you can view the workspace information, such as the workspace name, project, and ID. On the **Tag Management** tab, you can manage tags. For details, see [Managing Workspace Tags](#).

----End

4.3.2 Editing a Workspace


Scenario

You can modify the workspace basic settings, including name, tag, and description.

This section describes how to edit a workspace.

Procedure

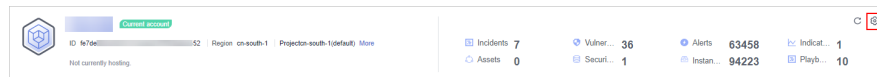
Step 1 Log in to the management console.

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

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

Step 4 Click  in the upper right corner of the target workspace.

Figure 4-2 Workspace details page



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

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

----End

4.3.3 Managing Workspace Tags

Scenario

After creating a workspace, you can add, edit, and delete tags configured for the workspace. A tag consists of a key-value pair. Tags are used to identify, and classify workspaces. Workspace tags are used for workspace management only.

If your organization has configured tag policies for SecMaster, add tags to workspaces based on the policies. If a tag does not comply with the tag policies, workspaces may fail to be created. Contact your organization administrator to learn more about tag policies.

This topic describes how to manage tags.

Limitations and Constraints

A maximum of 20 tags can be added for a workspace.

Procedure



- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**.
- Step 4** Click  in the upper right corner of the target workspace.

Figure 4-3 Workspace details page



- Step 5** On the workspace details page, choose **Tag Management**.
- Step 6** On the **Tag Management** page, manage tags.

Table 4-3 Managing tags

Operation	Description
Adding a tag	<ol style="list-style-type: none"> On the Tag Management tab, click Add Tag. In the displayed Add Tag tab, configure the tag key and value. Click OK.
Editing a tag	<ol style="list-style-type: none"> On the Tag Management tab, locate the row that contains the target tag and click Edit in the Operation column. In the displayed Edit Tag dialog box, change the tag value. Click OK.
Deleting a tag	<p>On the Tag Management tab, locate the row that contains the target tag and click Delete in the Operation column. In the displayed Delete Tag dialog box, click OK.</p>

----End

4.3.4 Deleting a Workspace

Scenario

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 part of the page and choose **Security > SecMaster**.

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


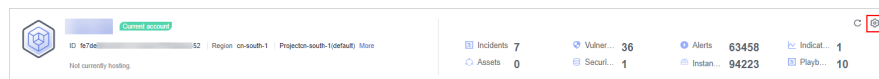
Step 4 Click  in the upper right corner of the target workspace.

Figure 4-4 Workspace details page



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

Step 6 In the **Delete Workspace** dialog box displayed, confirm the information, select **Permanently delete the workspace**, and enter the workspace name in the **Confirm Deletion** text box. Then, click **Delete**.

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.

----End

5 Viewing Purchased Resources

Scenario

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 part 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.

Table 5-1 Parameters for purchased resources

Parameter	Description
Total/Subscribed Regions	Regions where SecMaster has been enabled for the current account and the total number of regions where SecMaster is rolled out.
Upgradeable	Number of resources that can be upgraded in all regions under the current account.
Versions About to Expire	The number of SecMaster editions and value-added packages that are about to expire in all regions under the current account.
Total Quota	The total quota you have under the current account in all regions.
Purchased Resources	Details about SecMaster resources you applied in each region. If there are many editions or regions, you can use filters to quickly search for a specified resource.


----End

6 Security Situation

6.1 Situation Overview

The **Situation Overview** page displays the overall security assessment status of resources in the current workspace in real time. You will view the security assessment results, security monitoring details, and security trend of your assets.

Procedure

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

The following table describes the reference periods and update frequency of the modules.

Table 6-1 Situation Overview

Parameter	Reference Period	Update Frequency	Description
Security Score	Real-time	<ul style="list-style-type: none"> Automatic update at 02:00 every day Updated every time you click Check Again 	The score is calculated based on what security services are enabled, and the levels and numbers of unhandled configuration issues, vulnerabilities, and threats. For details, see Security Scores and Unscored Items .
Threat Alarms	Last 7 days	Every 5 minutes	Total number of alerts on the Threat Operations > Alerts page in a workspace.
Vulnerabilities	Last 7 days	Every 5 minutes	Total number of vulnerabilities on the Risk Prevention > Vulnerabilities in a workspace.
Abnormal Baseline Settings	Real-time	Every 5 minutes	Total number of issues on the Risk Prevention > Baseline Inspection page in a workspace.
Your Security Score over Time	Last 7 days	Every 5 minutes	Security scores in the last seven days.

----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.

- The security score is automatically updated at 02:00 every day. You can also click **Check Again** to update it immediately.
- 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:**
 - i. In the **Security Score** area, click **Handle Now**.
 - ii. On the **Risks** slide-out panel displayed, click **Handle**.
 - iii. 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 six 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**.
 - If you have fixed asset risks and refreshed the alert status, you can click **Check Again** to update the security score.

 **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 6-2 Security score table

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

- Unscored Check Items

Table 6-3 lists the security check items and corresponding points.

Table 6-3 Unscored check items

Category	Unscored Item	Unscored Point	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		

Category	Unscored Item	Unscored Point	Suggestion	Maximum Unscored Point
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.

Table 6-4 Security Monitoring parameters

Parameter	Description
Threat Alarms	<p>This panel displays the unhandled threat alerts in a workspace 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. The statistics are updated every 5 minutes.</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 in a workspace 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. The statistics are updated every 5 minutes.</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 the five vulnerability types with the most affected servers. <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 in a workspace. You can quickly learn of total number of violations and the number of violations at each severity level. The statistics are updated every 5 minutes.</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, 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. - 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**. The statistics are updated every 5 minutes.

6.2 Large Screen


6.2.1 Overall Situation Screen

Scenarios

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Situation > Large Screen**.
- Step 5** Click **Play** in the lower right corner of the comprehensive situation awareness image to access the screen.

This screen includes many graphs. More details are provided below.

----End

Security Score

The security score of the current assets is displayed.

Table 6-5 Security Score

Parameter	Reference Period	Update Frequency	Description
Security Score	Real-time	<ul style="list-style-type: none"> Automatic update at 02:00 every day Updated about 5 minutes after you click Check Again in the Security Score panel on the Situation Overview page in a workspace. 	<p>The score is calculated based on what security services are enabled, and the levels and numbers of unhandled configuration issues, vulnerabilities, and threats. Each calculation item is assigned a weight.</p> <ul style="list-style-type: none"> There are six 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.

To view details about the alert statistics, choose **Threat Operations > Alerts** in the current workspace.

Table 6-6 Alert statistics

Parameter	Reference Period	Update Frequency	Description
New Alerts	Today	5 minutes	Number of new alerts generated on the current day.
Threat Alerts	Last 7 days	5 minutes	Number of new alerts generated in the last seven days.

Parameter	Reference Period	Update Frequency	Description
Unhandled Alerts	Last 7 days	5 minutes	Number of alerts that have not been cleared in the last seven days.
Handled Alerts	Last 7 days	5 minutes	Number of alerts that have been cleared in the last seven days.

Asset Protection

The protection status of servers and websites is displayed, including the proportion of protected and unprotected assets. You can hover the cursor over a module to view the number of protected/unprotected assets.

Table 6-7 Asset protection rate

Parameter	Reference Period	Update Frequency	Description
Asset Protection (%)	Last 7 days	5 minutes	<p>The protection status of servers and websites is displayed, including the proportion of protected and unprotected assets.</p> <ul style="list-style-type: none"> • Servers: numbers of ECSs protected and not protected by HSS • Websites: Numbers of websites protected and not protected by WAF

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.

- To view details about the baseline data, choose **Risk Prevention > Baseline Inspection** in the current workspace.
- To view details about the vulnerability data, choose **Risk Prevention > Vulnerabilities** in the current workspace.

Table 6-8 Baseline inspection

Parameter	Reference Period	Update Frequency	Description
Baseline Settings	Real-time	5 minutes	Numbers of baseline settings that passed and failed the last baseline inspection.
Vulnerabilities	Last 7 days	5 minutes	Numbers of fixed and unfixed vulnerabilities in the last seven days.
Resources by Severity	Real-time	5 minutes	Numbers of unsafe resources at different severities in the last baseline inspection. Severity: Critical, High, Medium, Low, and Info.
Vulnerabilities	Last 7 days	5 minutes	New vulnerabilities by the day for the last seven days and vulnerability distribution.

Recent Threats

The numbers of threatened assets and security logs reported every day in the last seven days are displayed.

The x-axis indicates time, the y-axis on the left indicates the number of threatened assets, and the y-axis on the right indicates the number of logs. Hover the cursor over a date to view the number of threatened assets of that day.

Table 6-9 Recent threats

Parameter	Reference Period	Update Frequency	Description
Attacks	Last 7 days	5 minutes	Number of alerts reported every day in the last seven days. To view details about the alert statistics, choose Threat Operations > Alerts in the current workspace.
Logs	Last 7 days	5 minutes	Number of security logs reported every day in the last seven days.

To-Dos

The to-do items in the current workspace are displayed.

Table 6-10 To-dos

Parameter	Reference Period	Update Frequency	Description
To-Dos	Real-time	5 minutes	To-do items on the Security Situation > Task Center in the current workspace.

Resolved Issues

The alert handling status, SLA and MTTR fulfillment rate in the last seven days, and automatic incident handling statistics in the last seven days are displayed.

To view details about the alert statistics, choose **Threat Operations > Alerts** in the current workspace.

Table 6-11 Resolved issues

Parameter		Reference Period	Update Frequency	Description
Alerts	Alerts	Last 7 days	5 minutes	Number of new alerts generated in the last seven days.
	Handled			Number of alerts that have been cleared in the last seven days.
	Manual			Number of alerts that were handled within the SLA time in the last seven days. Alerts handled as planned and earlier than planned are counted.
	Auto			Number of alerts that were automatically handled by SecMaster playbooks over the past seven days. To determine how an alert was handled, check whether the value of close_comment is ClosedByCSB or ClosedBySecMaster in the alert details. If it is, the alert was automatically handled. If it is not, the alert was manually handled.

Parameter		Reference Period	Update Frequency	Description
SLA and MTTR [Last 7 Days]	SLA Statistics	Last 7 days	5 minutes	<p>Alert handling timeliness in the last seven days. The formula is as follows: For an alert with Service-Level Agreement (SLA) specified, if Alert closure time - Alert generation time \leq SLA, it indicates the alert was handled in a timely manner. Otherwise, the alert fails to meet SLA requirements.</p> <ul style="list-style-type: none"> Compliant: The alert closure time is the same as or earlier than planned. Non-compliant: The alert closure time is later than planned.
	MTTR			<p>Average alert closure time in the last seven days. The formula is as follows: Mean Time To Repair (MTTR) = Total processing time of each alert/Total number of alerts. Processing time of each alert = Closure time - Creation time.</p>
Handled Alerts [Last 7 Days]		Last 7 days	5 minutes	<p>Total number of alerts handled in the last seven days.</p> <ul style="list-style-type: none"> Manual: Number of alerts manually closed on the Alerts page. Auto: Number of alerts automatically closed by SecMaster playbooks. <p>To determine how an alert was handled, check whether the value of close_comment is ClosedByCSB or ClosedBySecMaster in the alert details. If it is, the alert was automatically handled. If it is not, the alert was manually handled.</p>

6.2.2 Security Response Screen


Scenarios

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 **Security Response** 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Situation > Large Screen**.
- Step 5** Click **Play** in the lower right corner of the security response image to access the screen.

This screen includes many graphs. More details are provided below.

----End

Monitoring Statistics Overview

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

Table 6-12 Security Response Overview

Parameter	Statistical Period	Update Frequency	Description
Unhandled Alerts	Last 7 days	5 minutes	Number of alerts to be handled in the last seven days. To view details about the alert statistics, choose Threat Operations > Alerts in the current workspace.
Unhandled Incidents	Last 7 days	5 minutes	Number of open or blocked incidents in the last seven days. To view details about the alert statistics, choose Threat Operations > Alerts in the current workspace.
Unhandled Vulnerabilities	Real-time	5 minutes	The number of unfixed vulnerabilities. To view details about the vulnerability data, choose Risk Prevention > Vulnerabilities in the current workspace.

Parameter	Statistica l Period	Update Frequenc y	Description
Unhandled Baseline Settings	Real-time	5 minutes	The number of items failed to pass the baseline inspection. To view details about the baseline data, choose Risk Prevention > Baseline Inspection in the current workspace.

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.

Table 6-13 Unhandled Alerts

Parameter	Statistica l Period	Update Frequenc y	Description
Unhandled Alerts	Last 7 days	5 minutes	Number of alerts that have not been handled for the last seven days. To view details about the alert statistics, choose Threat Operations > Alerts in the current workspace.

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.

Table 6-14 Unhandled Incidents

Parameter	Statistica l Period	Update Frequenc y	Description
Unhandled Incidents	Last 7 days	5 minutes	Number of incidents that have not been closed in the last seven days. To view details about the alert statistics, choose Threat Operations > Alerts in the current workspace.

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.

Table 6-15 Unhandled Vulnerabilities

Parameter	Statistica l Period	Update Frequenc y	Description
Unhandled Vulnerabilities	Last 7 days	5 minutes	The number of unfixed vulnerabilities. To view details about the vulnerability data, choose Risk Prevention > Vulnerabilities in the current workspace.

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.

Table 6-16 Unhandled Baseline Settings

Parameter	Statistics Cycle	Update Frequency	Description
Unhandled Baseline Settings	Last 7 days	5 minutes	The number of items failed to pass the baseline inspection. To view details about the baseline data, choose Risk Prevention > Baseline Inspection in the current workspace.


6.2.3 Asset Security Screen

Scenarios

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Situation > Large Screen**.
- Step 5** Click **Play** in the lower right corner of the **Asset Security Situation** screen to access the page.

This screen includes many graphs. More details are provided below.

----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 in the current workspace.

Table 6-17 Asset Security Screen

Parameter	Statistical Period	Update Frequency	Description
Assets	Real-time	Hourly	Total number of assets managed in Resource Manager .
Attacked Assets	Last 7 days	Hourly	Number of assets affected by alerts aggregated in Alerts under Threat Operations in the current workspace.
Unprotected Assets	Real-time	Hourly	<p>Number of assets for which security protection is not enabled, for example, ECSs for which HSS is not enabled and EIPs for which DDoS is not enabled. You will learn of how many assets with Protection Status marked as Unprotected in Resource Manager.</p> <p>In Resource Manager, the protection status for assets is as follows:</p> <ul style="list-style-type: none"> ● Protected: The security product required for an asset is enabled for the asset. ● Unprotected: The security product required for an asset has not been purchased or enabled for the asset. If you want to protect target assets, purchase corresponding security products and enable protection. For example, if you want to protect ECSs, purchase HSS and enable HSS for each ECS. ● --: The required security product is not supported in the current region.
Assets with Vulnerabilities or Unsafe Settings	Real-time	Hourly	<p>These assets include assets affected by vulnerabilities and assets have unsafe settings discovered during baseline inspection. The duplicated assets are counted only once.</p> <p>The vulnerability data comes from Risk Prevention > Vulnerabilities, and the baseline inspection data comes from Risk Prevention > Baseline Inspection > Resources to Check.</p>

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.

Table 6-18 Asset Distribution

Parameter	Statistical Period	Update Frequency	Description
Assets by Type	Real-time	Hourly	Number of different types of assets in Resource Manager .
Protection by Asset Type (%)	Real-time	Hourly	Percentage of protection for different types of assets. Protection rate of a certain type of assets = Protected assets/Total number of assets of this type.
Asset Changes	Last 7 days	Hourly	Statistics on the total number of assets, and the number of assets with vulnerabilities and unsafe settings in the last seven days.
Top 5 Attacked Assets	Last 7 days	Hourly	Top 5 attacked assets in the last seven days and the number of attacks. The data comes from Threat Operations > Alerts . You can view details on this page.

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.

Table 6-19 Top 5 Assets with the Most Vulnerabilities and Top 5 Departments with the Highest Protection Rate

Parameter	Statistical Period	Update Frequency	Description
Top 5 Assets with the Most Vulnerabilities	Real-time	Hourly	<p>Top 5 assets with the most vulnerabilities in different departments.</p> <p>This data is generated based on the assets affected by vulnerabilities in Risk Prevention > Vulnerabilities. Note that the assets must have department details provided, or the affected assets may fail to be counted toward this data.</p>
Top 5 Departments with the Highest Protection Rate	Real-time	Hourly	<p>This graphs list the 5 departments that have the highest protection rate, in descending order.</p> <p>Note that the assets on Resource Manager must have department details provided, or the assets cannot be counted toward this rate.</p>


6.2.4 Threat Situation Screen

Scenarios

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** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** Click **Play** in the lower right corner of the **Threat Situation** screen to access the page.

This screen includes many graphs. More details are provided below.

----End

Threat Situation screen

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

Table 6-20 Threat Situation screen

Parameter		Statistical Period	Update Frequency	Description
Network Attacks	<i>Occurrences</i>	Last 7 days	Hourly	The number of attacks against EIPs in the last seven days.
	Last Week			Difference between the number of attacks against EIPs for the current 7-day statistical cycle and that for the previous 7-day statistical cycle.
Application Attacks	<i>Occurrences</i>	Last 7 days	Hourly	The number of attacks against protected websites in the last seven days.
	Last Week			Difference between the number of attacks against websites for the current 7-day statistical cycle and that for the previous 7-day statistical cycle.
Server Attacks	<i>Occurrences</i>	Last 7 days	Hourly	The number of attacks against protected ECSs in the last seven days.
	Last Week			Difference between the number of attacks against ECSs for the current 7-day statistical cycle and that for the previous 7-day statistical cycle.

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.

Table 6-21 Attack source distribution

Parameter	Statistica l Period	Update Frequenc y	Description
Top 5 Network Attack Source Distribution	Last 7 days	Hourly	The five sources that have launched the most attacks against EIPs for the last seven days, displayed in a descending order by attack quantity.
Top 5 Application Attack Source Types	Last 7 days	Hourly	The five sources that have launched the most attacks against websites for the last seven days, displayed in a descending order by attack quantity.

Attacks by Type

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

Table 6-22 Attacks by Type

Parameter	Statistica l Period	Update Frequenc y	Description
Top 5 Network Attack Types	Last 7 days	Hourly	The five attack types with the most attacks against EIPs detected for the last seven days, displayed in a descending order by attack quantity. If there is no network attack or no corresponding data table, the default types with zero attacks are displayed.
Top 5 Application Attack Types	Last 7 days	Hourly	The five attack types with the most attacks against websites detected for the last seven days, displayed in a descending order by attack quantity. If there is no application attack or no corresponding data table, the default types with zero attacks are displayed.

Parameter	Statistical Period	Update Frequency	Description
Top 5 Server Attack Types	Last 7 days	Hourly	<p>The five attack types with the most attacks against ECSs detected for the last seven days, displayed in a descending order by attack quantity.</p> <p>If there is no ECS attack or no corresponding data table, the default types with zero attacks are displayed.</p> <p>The asset statistics come from the Alerts page under Threat Operations in the current workspace.</p>

Threat Situation Statistics

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

Table 6-23 Threat Situation Statistics

Parameter		Statistical Period	Update Frequency	Description
Alert Statistics	Logs	Last 7 days	Hourly	Total number of network, application, and server access logs for the last seven days.
	Threats			Total number of threats identified for protected networks, applications, and servers for the last seven days.
	Alerts			This number reflects alerts collected in Threat Operations > Alerts for the last seven days.
	Incidents			This number reflects incidents collected in Threat Operations > Incidents for the last seven days.
Log Analysis	Log volume	Last 7 days	Hourly	Total volume of network, application, and server access logs for the last seven days, in MB.

Parameter		Statistical Period	Update Frequency	Description
	PoP			Difference between the total volume of network, application, and server access logs for the current 7-day statistical cycle and that for the previous 7-day statistical cycle. Calculation method: [(Number of logs for the current statistical cycle – Number of logs for the previous statistical cycle)/Number of logs for the previous statistical cycle] x 100%.
	Statistical trend chart			Total volume of network, application, and server access logs for the last seven days, in MB.
Threats by Model	Models	Real-time	Hourly	The number includes the models in Threat Operations > Intelligent Modeling .
	Statistical table	Last 7 days	Hourly	Number of threats detected by each type of threat detection model. If there is no threat detection model, four default types with zero threats detected are displayed.


6.2.5 Vulnerability Situation Screen

Scenarios

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 vulnerability situation 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

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

Step 5 Click **Play** in the lower right corner of the **Vulnerability Situation** image to access the page.

This screen includes many graphs. More details are provided below.

----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.

Table 6-24 Vulnerable Assets Overview

Parameter	Statistical Period	Update Frequency	Description
Vulnerable Assets	Real-time	Hourly	The number of assets with vulnerabilities or risky baseline settings.
Vulnerabilities	Real-time	Hourly	Vulnerabilities collected in Vulnerabilities .
Risky Baseline Settings	Real-time	Hourly	Data reported by Baseline Inspection in SecMaster.
Unprotected Assets	Real-time	Hourly	Number of assets for which you need to enable security protection, for example, ECSs for which HSS is not enabled and EIPs for which DDoS mitigation is not enabled.

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.

Table 6-25 Vulnerable departments

Parameter	Statistica l Period	Update Frequenc y	Description
Top 5 Vulnerable Departments	Real-time	Hourly	The five departments have the most vulnerable assets, assets affected by vulnerabilities, and unprotected assets. Vulnerable assets include assets affected by vulnerabilities in Risk Prevention > Vulnerabilities , and assets that fail any check in Risk Prevention > Baseline Inspection , and assets that are not protected in Resource Manager . Note that the assets in Resource Manager must have department details provided, or they cannot be counted in calculation.

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.

Table 6-26 Department with the most unprotected assets

Parameter	Statistica l Period	Update Frequenc y	Description
Top 5 Department with the Most Unprotected Assets	Real-time	Hourly	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.

Table 6-27 Vulnerability fix rate

Parameter	Statistical Period	Update Frequency	Description
Vulnerability Fix Rate	Real-time	Hourly	Vulnerability fixing rate = (Number of fixed vulnerabilities/Total number of vulnerabilities) x 100%. If no vulnerability exists, 100% is displayed.
Vulnerability Types	Real-time	Hourly	Vulnerabilities are displayed by vulnerability type.
Vulnerability Changes	Last 7 days	Hourly	Vulnerabilities in the last seven days are classified and counted by severity.

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.

Table 6-28 Baseline Inspection Pass Rate

Parameter	Statistical Period	Update Frequency	Description
Baseline Inspection Pass Rate	Real-time	Hourly	Baseline check pass rate = (Number of passed baseline check items/Total number of check items) x 100%.
Failed Checks By Type	Real-time	Hourly	Failed baseline check items are displayed by risk severity.
Baseline Inspection	Real-time	Hourly	This graph shows how many qualified, risky, and unqualified settings, respectively, discovered by baseline inspection.

6.3 Security Reports

6.3.1 Creating and Copying a Security Report

Scenario

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


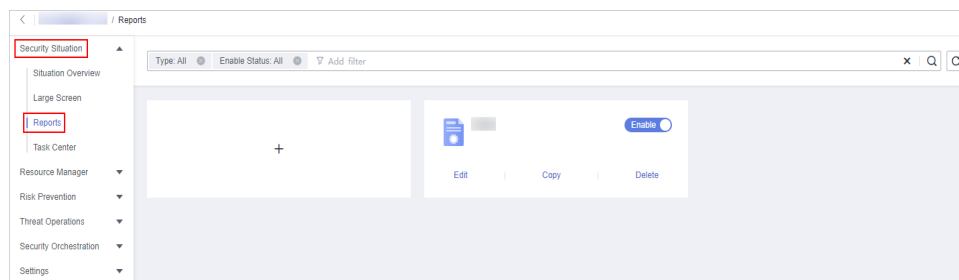
- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Situation > Security Reports**.

Figure 6-1 Reports




- Step 5** On the **Reports** page, click  to go to the basic configuration page.
- Step 6** Configure basic information of the report.



Table 6-29 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 00:00:00 to 23:59:59 of the previous day by default. ● Weekly: SecMaster collects statistics on security information from 00:00:00 on Monday to 23:59:59 on Sunday of the previous week. ● Monthly: SecMaster collects statistics on security information from 00:00:00 on the first day to 23:59:59 on the last day of the previous month. ● Custom: Customize a time range.
Data Scope	If you select the daily, weekly, or monthly schedule, the data scope is specified by default. If you select the custom schedule, you need to specify a data scope.

- Step 7** Click **Next: Report Choose** in the upper right corner.

Step 8 On the **Report Selection** page, select a report from the left. After selecting, you can preview the report layout in the right pane.

You need to select the corresponding report layout based on what you select for **Schedule**.


- To download a report, click  in the upper left corner of the report preview page. In the dialog box displayed, select a report format and click **OK**.
The system then automatically downloads the report for you.
- To view a report in full screen, click  in the upper left corner of the report preview page.

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

----End

Copying a Report

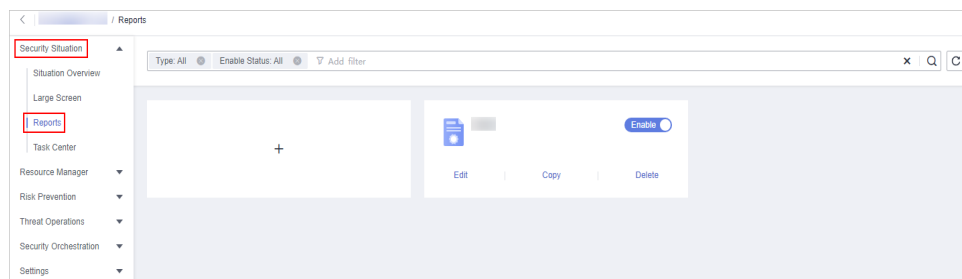
Step 1 Log in to the management console.

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

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

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



Figure 6-2 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.

- To download a report, click  in the upper left corner of the report preview page. In the dialog box displayed, select a report format and click **OK**.
The system then automatically downloads the report for you.
- To view a report in full screen, click  in the upper left corner of the report preview page.

Step 8 Click **Complete** in the lower right corner. On the displayed **Security Reports** page, view the newly created report.

----End


6.3.2 Viewing a Security Report

Scenario

This section describes how to view a created security report and its displayed information.

Procedure

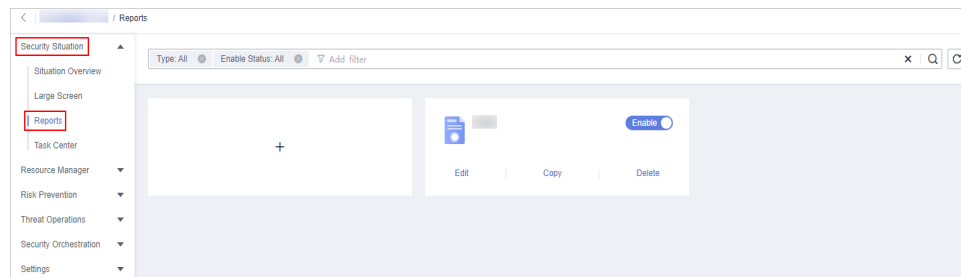
Step 1 Log in to the management console.

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

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

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

Figure 6-3 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.

----End

Content in the Daily Report Template

Table 6-30 Content in the daily report template

Parameter	Description
Data Scope	The default data scope of a daily report is from 00:00:00 to 23:59:59 on the previous day.

Parameter	Description
Security Score	SecMaster evaluates and scores your asset security for the previous day (from 00:00:00 to 23:59:59) 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 Inspection	<p>Displays the statistics of the latest baseline check, including the following information:</p> <ul style="list-style-type: none"> ● The number of baseline check items ● Number of failed compliance check items in the latest baseline check
Security Vulnerabilities	<p>Displays the vulnerability statistics of the accessed cloud services on the previous day, including the following information:</p> <ul style="list-style-type: none"> ● Number of vulnerabilities ● Number of unfixed vulnerabilities
Policy Coverage	<p>Displays the coverage of current security products, including the following information:</p> <ul style="list-style-type: none"> ● Number of instances protected by security products (= Number of protected ECSs + Number of websites protected with WAF instances) ● HSS coverage (= Number of protected ECSs/Total number of ECSs) ● Number of protected cloud servers ● Protected websites
Asset Security	<p>Displays the current asset security status, including the following information:</p> <ul style="list-style-type: none"> ● Total number of current assets ● Number of vulnerable assets
Security Analysis	<p>Displays the security analysis statistics of the previous day, including the following information:</p> <ul style="list-style-type: none"> ● Total traffic of security logs on the previous day ● Number of security log models
Security Response (Overview)	<p>Displays the security response statistics for the previous day, including the following information:</p> <ul style="list-style-type: none"> ● Number of security alerts handled ● Number of confirmed intrusion incidents ● Number of executed automatic response playbooks ● Percentage of alerts handled by automatic playbooks ● Average MTTR ● Number of confirmed high-risk intrusion incidents

Parameter	Description
Asset risks	<p>Displays the asset security status for the previous day, including the following information:</p> <ul style="list-style-type: none"> ● Number of attacked assets ● Number of unprotected assets ● Number of vulnerable assets ● Asset change trend over the last seven days as of the previous day ● Asset protection rate
Threat posture	<p>Displays the threat posture of assets on the previous day, including the following information:</p> <ul style="list-style-type: none"> ● Number of DDoS attacks ● Number of network attacks ● Number of application attacks ● Number of server attacks ● DDoS inspection findings ● Network and server attack changes ● WAF inspection findings ● Top 5 network attack types ● Top 5 application attack type statistics ● Top 5 server attack type statistics ● Top 5 application attack sources distribution ● Top 5 attacked application distribution ● Top 5 server alert distribution ● Top 5 network attack sources distribution ● HSS inspection findings
Log analysis	<p>Displays the log analysis results for the previous day, including the following information:</p> <ul style="list-style-type: none"> ● Number of log sources on the previous day ● Number of log indexes on the previous day ● Total number of logs received on the previous day ● Log volume stored on the previous day ● Log change trend over the last seven days as of the previous day ● Access traffic statistics of top 5 log sources over the last seven days as of the previous day ● Number of alerts generated by top 10 models on the previous day

Parameter	Description
Security Response (Details)	<p>Displays the security response information for the previous day, including the following information:</p> <ul style="list-style-type: none"> • Number of alerts handled on the previous day • Number of incidents handled on the previous day • Number of vulnerabilities fixed on the previous day • Number of unsafe baseline settings fixed on the previous day • Threat alert distribution and quantity on the previous day • Top 5 intrusion incidents by type on the previous day • Top 5 emergency responses on the previous day • Top 20 threat alerts handled on the previous day
External Security Info	<p>Displays information about external security hotspots for the previous day.</p>

Content in the Weekly Report Template

Table 6-31 Content in the **Weekly** Report Template

Parameter	Description
Data Scope	<p>SecMaster collects security information from 00:00:00 on Monday to 23:59:59 on Sunday of the previous week.</p>
Security Score	<p>SecMaster evaluates and scores your asset security for the last day of the previous week so that you can quickly learn of the overall security posture of assets. This score varies depending on the SecMaster edition you are using.</p>
Baseline Inspection	<p>Displays the statistics of the latest baseline check in the previous week, including the following information:</p> <ul style="list-style-type: none"> • The number of baseline check items • Number of compliance check items in the latest baseline check
Security vulnerabilities	<p>Displays the vulnerability statistics of the accessed cloud services for the last week, including the following information:</p> <ul style="list-style-type: none"> • Number of vulnerabilities. • Number of unfixed vulnerabilities

Parameter	Description
Policy Coverage	<p>Displays the latest asset security information on the last day of the previous week, including the following information:</p> <ul style="list-style-type: none"> ● Number of instances protected by security products (= Number of protected ECSs + Number of websites protected with WAF instances) ● HSS coverage (= Number of protected ECSs/Total number of ECSs) ● Number of protected cloud servers ● Protected websites
Asset security	<p>Displays the latest asset security information on the last day in the last week, including the following information:</p> <ul style="list-style-type: none"> ● Total number of assets ● Number of vulnerable assets
Security analysis	<p>Displays the security analysis statistics, including the following information:</p> <ul style="list-style-type: none"> ● Total security log traffic of last week ● Number of security log models on the last day of the last week
Security Response (Overview)	<p>Displays the security response information for the previous week, including the following information:</p> <ul style="list-style-type: none"> ● Number of security alerts handled over the previous week ● Number of confirmed intrusion incidents over the previous week ● Number of executed automatic response playbooks ● Percentage of alerts handled by automatic playbooks ● Average MTTR ● Number of confirmed high-risk intrusion incidents
Asset risks	<p>Displays the latest asset security information on the last day of the previous week, including the following information:</p> <ul style="list-style-type: none"> ● Week-over-week changes on attacked asset quantity in monthly reports ● Week-over-week changes on unprotected asset quantity in monthly reports ● Week-over-week changes on vulnerable asset quantity in monthly reports ● Asset changes over the previous week ● Asset protection (%)

Parameter	Description
Threat posture	<p>Displays the latest threat posture on the last day of the previous week, including the following information:</p> <ul style="list-style-type: none"> ● Number of DDoS attacks ● Number of network attacks ● Number of application attacks ● Number of server attacks ● DDoS inspection findings ● Network attack changes ● WAF inspection findings ● Top 5 network attack types ● Top 5 application attack types ● Top 5 server attack types ● Top 5 application attack sources distribution ● Top 5 attacked application distribution ● Top HSS alert distribution ● Top 5 network attack sources distribution ● HSS inspection findings
Log analysis	<p>Displays the log analysis results for the previous week, including the following information:</p> <ul style="list-style-type: none"> ● Number of log sources ● Number of log indexes ● Total number of received logs ● Log storage ● Log volume changes ● Top 5 log source access statistics ● Number of alerts generated by top 10 models on the previous day
Security Response (Details)	<p>Displays the security response information for the previous week, including the following information:</p> <ul style="list-style-type: none"> ● Number of handled alerts ● Number of handled incidents ● Number of fixed vulnerabilities ● Number of fixed baseline settings ● Threat alert distribution and quantity ● Top 5 intrusion incidents by type ● Top 5 emergency responses ● Top 20 threat alert handling
External Security Info	<p>This part includes information about external security hotspots.</p>

Content in the Monthly Report Template

Table 6-32 Content in the monthly report template

Parameter	Description
Data Scope	By default, a monthly report includes security information for the previous month.
Security Score	SecMaster evaluates and scores your asset security for the last day of the previous month 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 Inspection	Displays the statistics of the latest baseline check in the previous month, including the following information: <ul style="list-style-type: none"> • The number of baseline check items • Number of compliance check items in the latest baseline check
Security Vulnerabilities	Displays the vulnerability statistics of the accessed cloud services on the last data of the previous month, including the following information: <ul style="list-style-type: none"> • Number of vulnerabilities • Number of unfixed vulnerabilities
Policy Coverage	Displays the latest asset security information on the last day of the last month, including the following information: <ul style="list-style-type: none"> • Number of instances protected by security products (= Number of protected ECSs + Number of websites protected with WAF instances) • HSS coverage (= Number of protected ECSs/Total number of ECSs) • Number of protected cloud servers • Protected websites
Asset Security	Displays the latest asset security information on the last day of the last month, including the following information: <ul style="list-style-type: none"> • Total number of assets • Number of vulnerable assets

Parameter	Description
Security analysis	Displays the security analysis statistics, including the following information: <ul style="list-style-type: none"> ● Total security log traffic of the last month ● Number of security log models on the last day of the last month
Security Response (Overview)	Displays the security response information for the previous month, including the following information: <ul style="list-style-type: none"> ● Number of security alerts handled over the previous month ● Number of confirmed intrusion incidents ● Number of executed automatic response playbooks ● Percentage of alerts handled by automatic playbooks ● Average MTTR ● Number of confirmed high-risk intrusion incidents
Asset risks	Displays the latest asset security information on the last day of the last month, including the following information: <ul style="list-style-type: none"> ● Attacked asset quantity changes compared to the previous month ● Unprotected asset quantity changes compared to the previous month ● Vulnerable asset quantity changes compared to the previous month ● Asset changes over the previous month ● Asset protection (%)

Parameter	Description
Threat posture	<p>Displays the latest threat posture n on the last day of the previous month, including the following information:</p> <ul style="list-style-type: none"> ● Number of DDoS attacks ● Number of network attacks ● Number of application attacks ● Number of server attacks ● DDoS inspection findings ● Network attack changes ● WAF inspection findings ● Top 5 network attack types ● Top 5 application attack types ● Top 5 server attack types ● Top 5 application attack sources distribution ● Top 5 attacked application distribution ● Top HSS alert distribution ● Top 5 network attack sources distribution ● HSS inspection findings
Log analysis	<p>Displays the log analysis results for the previous month, including the following information:</p> <ul style="list-style-type: none"> ● Number of log sources ● Number of log indexes ● Total number of received logs ● Log storage ● Log volume changes ● Top 5 log source access statistics ● Number of alerts generated by top 10 models on the previous day
Security Response (Details)	<p>Displays the security response information for the previous month, including the following information:</p> <ul style="list-style-type: none"> ● Number of handled alerts ● Number of handled incidents ● Fixed vulnerabilities ● Number of fixed baseline settings ● Threat alerts by severity ● Top 5 intrusion incidents by type ● Top 5 emergency responses ● Top 20 threat alert handling

Parameter	Description
External Security Info	This part includes information about external security hotspots.

6.3.3 Downloading a Security Report

Scenario

You can download historical reports.

This topic describes how to download a report.

Procedure


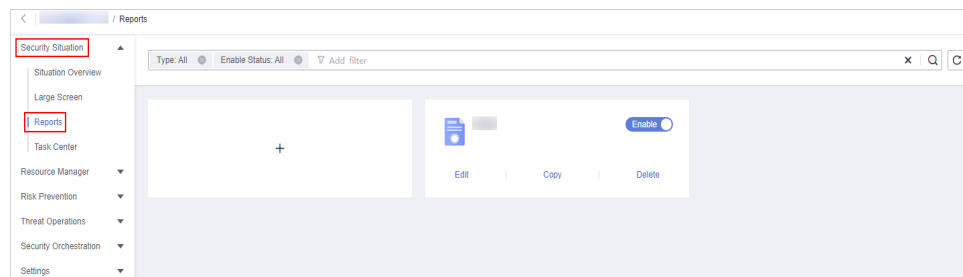

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Situation > Security Reports**.

Figure 6-4 Reports



- Step 5** Locate a report template and click **Edit**.
You can also download the report. For details, see [Creating and Copying a Security Report](#).
- Step 6** Click **Next: Report Choose** in the upper right corner. The **Report Selection** page is displayed.
- Step 7** On the report selection page, click  in the upper left corner of the preview page on the right.
To change the report schedule, edit it in the upper right corner of the preview page on the right.
- Step 8** In the displayed dialog box, select a report format, and click **OK**.

The system automatically downloads the report to the local PC.

----End

6.3.4 Managing Security Reports

Scenario

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

Procedure


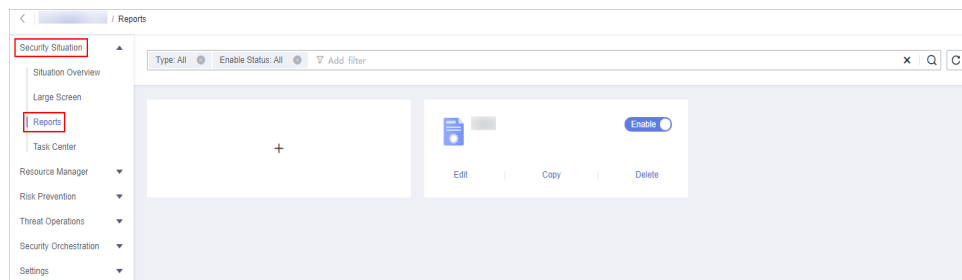
- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Situation > Security Reports**.

Figure 6-5 Reports



- Step 5** Manage security reports.

Table 6-33 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.

Operation	Step
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

6.4 Task Center

6.4.1 Viewing To-Do Tasks

Scenario

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Situation > Task Center**.
- Step 5** On the **To-Dos** tab page displayed, view details about the to-do tasks.

Table 6-34 To-do task parameters

Parameter	Description
Task Name	Name of a task.
Service Type	Type of a task. <ul style="list-style-type: none"> • Workflow release • Playbook release • Playbook - Node Review

Parameter	Description
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
Remarks	Remarks of a task.
Created	Time when the playbook or process is created.
Updated	Last update time of the playbook or process.
Expired	Time the task expires.
Operation	Approve the to-do task.

----End

6.4.2 Handling a To-Do Task

Scenario

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 part of the page and choose **Security > SecMaster**.

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

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

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


6.4.3 Viewing Completed Tasks

Scenario

This section walks you through how to view tasks you have handled in SecMaster.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Situation > Task Center**. On the displayed page, click the **Completed** tab.

Step 5 View details about handled tasks in the task list.

If there are many completed tasks, you can select a filter, enter a keyword in the search box, and press **Enter** to quickly find the one you want.

Table 6-35 Completed task parameters

Parameter	Description
Task	Name of a task.
Work	Type of a task. <ul style="list-style-type: none"> • Workflow release • Playbook release • Playbook - Node review
Object	Name of the corresponding playbook or workflow.
Created By	User who creates the task.
Remarks	Remarks of the task.
Reviewed By	Reviewer of the playbook/workflow
Comment	Review comment of the task.
Description	Description of the task.
Created	Time when the playbook or workflow was created.
Updated	Last time the playbook or workflow was updated.

Parameter	Description
Expired	Time the task expires.

----End

7 Resource Manager

7.1 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.

7.2 Configuring the Asset Subscription

Scenario


SecMaster can synchronize asset information only in the workspace where asset subscription is enabled. After the subscription, SecMaster updates resource information every night.

This section describes how to make a subscription to resources.

NOTE

- Only cloud resources can be subscribed to and synchronized to SecMaster. Subscribing to resource information to multiple workspaces in a region is not recommended.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Resource Manager > Resource Manager**.

- Step 5** On the **Resource Manager** page, click **Asset Subscription** in the upper right corner.
- Step 6** On the **Asset Subscription** page sliding out from the right, locate the row that contains the region where the target resource is located, and enable subscription.
- Step 7** Click **OK**.
- After the subscription, SecMaster updates resource information every night.
- End

7.3 Viewing Resource Information


Scenario

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

Prerequisites

- You have completed asset subscriptions. For details, see [Configuring the Asset Subscription](#).

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Resource Manager > Resource Manager**.
- Step 5** (Optional) Complete the asset subscription first. If you have done this once, skip this step.

SecMaster can synchronize asset information only in the workspace where asset subscription is enabled. After the subscription, SecMaster updates resource information every night.

NOTE

Only cloud resources can be subscribed to and synchronized to SecMaster. Subscribing to resource information to multiple workspaces in a region is not recommended.

- On the **Resource Manager** page, click **Asset Subscription** in the upper right corner.
 - On the **Asset Subscription** page sliding from the right, locate the row that contains the region where the target resource is located, and enable subscription.
 - Click **OK**.
- After the subscription, SecMaster updates resource information every night.

Step 6 On the displayed page, view the resource details.

- You can view resource information by resource type. For example, you can select the **Servers** tab to view details about servers you have.
- If there are many resources displayed, use filters to search for a specific resource.

To view the asset information of an enterprise project, select the enterprise project name to filter.

- You can view the total number of assets below the asset list. You can view a maximum of 10,000 asset records page by page. To view more than 10,000 asset records, optimize the filter criteria.
- To view more details about an asset, check its asset type. Then, go to the corresponding resource tab and click the resource name of the asset to go to its details page.

For example, to view details about a server, select the **Servers** tab. On the displayed tab, click the resource name of the target server to go to its details page.

- On the asset details page, you can view the environment, asset, and network details related to the asset.
- Edit the owner, service system, and department of the resource. You can also bind the resources to or unbind the resources from an owner, service system, or department.

----End

Related Operations

On the **Resource Manager** page, you can edit the department, service system, and owner of a resource. Perform the following steps:

1. Select the resources you want to edit click **Batch Edit** in the upper left corner of the resource list.
2. In the displayed box, edit resource details.
3. Click **OK**.

7.4 Importing and Exporting Assets

Scenario


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 5 MB can be imported.
- A maximum of 9,999 resource records can be exported.

Importing Assets

- Step 1** Log in to the management console.
 - Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
 - Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
 - Step 4** In the navigation pane on the left, choose **Resource Manager > Resource Manager**.
 - Step 5** On the **Resource Manager** page, click a tab corresponding to the type of the resources you want to import. For example, if you want to import servers, click the **Servers** tab.
 - 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.
 - Step 8** After the template is completed, click **Select File** in the **Import** dialog box and select the Excel file you want to import.
 - Step 9** Click **OK**.
- End

Exporting Assets



- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Resource Manager > Resource Manager**.
- Step 5** On the asset management page, click the corresponding asset tab. For example, if you want to export servers, click the **Servers** 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 7-1 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

7.5 Editing and Deleting Resources

Scenario

On the **Resource Manager** page, you can edit the department, service system, and owner of a resource. You can also delete resources you imported into SecMaster.


This topic describes how to edit or delete a resource from SecMaster.

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 part of the page and choose **Security > SecMaster**.

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

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

Step 5 Edit or delete the resource.

Table 7-2 Parameters for resource edit or deletion

Operation	Procedure
Batch Edit	<ol style="list-style-type: none"> On the Resource Manager page, select the resources you want to edit and click Batch Edit in the upper left corner of the resource list. To edit a resource of a certain type, click the corresponding resource type tab. For example, if you want to edit servers, click the Servers tab. In the displayed box, you can edit the department, service system, and owner of the resource. Click OK.

Operation	Procedure
Batch Delete	<ol style="list-style-type: none"> 1. On the Resource Manager page, click the corresponding resource type tab. For example, if you want to delete servers, click the Servers tab. 2. On the displayed page, select the resources you want to delete and click Batch Delete above the list. The system will delete all selected resources.

----End

8 Risk Prevention

8.1 Baseline Inspection

8.1.1 Baseline Inspection Overview

SecMaster 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.

Baseline Check Methods

- Automated baseline checks
By default, SecMaster performs a check every three days. From 00:00 to 06:00, SecMaster checks all assets in the current region under your account based on compliance pack **Cloud Security Compliance Check 1.0**.
You can specify a schedule and start time to let SecMaster perform baseline inspection. For details, see [Creating a Custom Check Plan](#).
- Manual baseline checks
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. For automatic check items, you can manually start specific checks.

Process

Table 8-1 Process

No.	Operation	Description
1	(Optional) Creating a Custom Baseline Check Plan	SecMaster uses the default check plan to check all assets. <ul style="list-style-type: none"> Default plan: SecMaster checks your assets under your account in the current region every three days from 00:00 to 06:00. Custom plans: SecMaster performs baseline inspections based on the compliance packs and time you specify in the custom check plans.
2	(Optional) Starting an Immediate Baseline Check	The baseline inspection supports periodic and immediate checks. <ul style="list-style-type: none"> Periodic check: The system automatically executes the default check plan or the check plans you configure. 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.
3	Viewing Baseline Inspection Results	You can view the baseline inspection results after each manual check or automated check. You can quickly learn affected assets and details about the baseline inspection items.
4	Handling Baseline Inspection Results	You can handle risky items based on the rectification suggestions.

8.1.2 Creating a Custom Check Plan

Scenarios

SecMaster can check whether your assets have risks based on baseline check plans. By default, every three days SecMaster automatically performs a baseline check on all assets in the current region under your account from 00:00 to 06:00 in accordance with compliance pack *Cloud Security Compliance Check 1.0*. You can also specify custom check periods and time.

This document describes how to create a custom baseline check plan.

Limitations and Constraints

- A compliance pack can be added to only one check plan.

- Check items in compliance pack **DJCP Level 3 Requirements** are manual check items. So, SecMaster does not support check plans that contain this package.
- The default check plan can be enabled or disabled only. No changes on its compliance packs or execution time can be made.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Plan** tab.
- Step 5** On the **Check Plan** tab, click **Create Plan**. The pane for creating a plan is displayed on the right.
- Step 6** Configure the check plan.

Table 8-2 Parameters for creating a check plan

Parameter		Description
Basic Information	Name	Custom 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
Select Compliance Pack		Select the compliance pack you want to use.

- 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

You can view, edit, enable, disable, or delete a custom check plan.

- Viewing a check plan

- a. In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the **Baseline Inspection** page, click the **Security Standards** tab. Then, click the **Check Plan** tab.
- b. On the **Check Plan** page, view what check plans you already have.
- Editing a custom check plan
Only custom check plans can be edited.
 - a. In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the **Baseline Inspection** page, click the **Security Standards** tab. Then, click the **Check Plan** tab.
 - 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. Edit settings and click **OK**.
- Deleting a custom check plan
Only custom check plans can be deleted.
 - a. In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the **Baseline Inspection** page, click the **Security Standards** tab. Then, click the **Check Plan** tab.
 - b. In the upper right corner of the check plan box, click **Delete**.
 - c. In the displayed dialog box, click **OK**.
- Disabling or enabling a check plan
 - a. In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the **Baseline Inspection** page, click the **Security Standards** tab. Then, click the **Check Plan** tab.
 - b. Toggle on or off the status button in the box where the target plan is located.

8.1.3 Starting an Immediate Baseline Check

Scenarios

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.
- **Immediate check:** You can start check items in all security standards or a specific check plan anytime.

This topic describes how to start an immediate baseline inspection. You can select the following check types:

- **Immediate Check on All Compliance Packs:** Check the compliance of all automatic check items in in-use compliance packs.
- **Starting a Check Based on a Check Plan:** Check the compliance of the check items in the compliance pack configured in a selected check plan.
- **Immediate Checks on Certain Check Items:** check the selected check items.


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.

Immediate Check on All Compliance Packs

This part describes how to start an immediate check for automatic check items in in-use compliance packs.

Step 1 Log in to the management console.

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

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

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

Step 5 On the **Check Result** tab, click **Check Now**. In the dialog box displayed, click **OK**.


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

This part describes how to immediately execute a check plan. Once a check plan is kicked off, SecMaster immediately executes each check item included in compliance packs in the check plan.

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Plan** tab.

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


SecMaster immediately executes the selected baseline check plan.

----End

Immediate Checks on Certain Check Items

This part describes how to start an immediate check on certain check items.

Step 1 Log in to the management console.

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

- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**.
- Step 5** Check one or more check items immediately.
- Check on a single check item
 - a. In the check item list in the lower part of the **Check Result** tab, locate the target automatic check item and click **Check Now** in the **Operation** column.
 - b. In the displayed dialog box, click **OK**.
Refresh the page and check the details next to **Last checked** and ensure that the latest scan result is displayed.
 - Checks on some check items
 - a. In the check item list in the lower part of the check result tab, select multiple auto check items and click **Check Now** in the upper left corner above the check item list.
 - b. In the displayed dialog box, click **OK**.
Refresh the page and check the details next to **Last checked** and ensure that the latest scan result is displayed.

----End

8.1.4 Viewing Check Results

Scenarios

After a check plan is set, you can perform an immediate check on the **Baseline Inspection** page. It takes about 10 minutes for the check results to be displayed on the result page. For details about how to perform an immediate check, see [Starting an Immediate Baseline Check](#).


If you do not perform an immediate check, the system performs the check at the specified time according to the check plan. For example, the system performs the check every three days by default, and the check is performed from 00:00 to 06:00 each time. You can view the check results on the **Check Result** page.

This topic describes where to view results of a baseline check plan.

Prerequisites

- Cloud service baseline scanning has been performed.

Procedure

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

Step 4 (Optional) In the navigation pane on the left, choose **Settings > Data Integration**. On the displayed page, locate the row that contains **Cloud Service Compliance Check** and enable **Compliance Baseline Log** in the **Logs** column.

SecMaster synchronizes all security data within a region to the first workspace in the region. For the non-first workspaces, you need to configure log access manually.

This topic describes how to enable log access to SecMaster manually.

After the setting is complete, you can start an immediate check on the **Baseline Inspection** page. It takes about 10 minutes for the check results to be displayed on the result page. For details about how to perform an immediate check, see [Starting an Immediate Baseline Check](#).

If you do not perform an immediate check, the system performs the check at the specified time according to the check plan. For example, the system performs the check every three days by default, and the check is performed from 00:00 to 06:00 each time. You can view the check results on the **Check Result** page.

Step 5 In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**.

Step 6 On the **Check Result** tab, view the check results of check items. For details about parameters, see [Table 8-3](#).

Table 8-3 Check result parameters

Parameter	Description
Risks By Severity	Risks found in the last baseline check are listed by severity as well as the corresponding resource quantity. Severity: Critical, High, Medium, Low, and Info.
Security Policy Check Results	This graph shows how many failed and passed check items your cloud services have in the last baseline check.
Security Standard Compliance Status	This part shows how well your workloads comply with each security standard. You will see a percentage of passed check items in total check items for each standard.
Pass Rate	Rate of the passed check items in the latest baseline check. Overall pass rate = Passed check items/Total check items. All check items in security standards used for the check plan executed are considered when the pass rate is calculated. The check result can be Passed, Failed, or Errors .

Parameter	Description
Security Standards and the check result list	<p>All security standards and check results are displayed.</p> <ul style="list-style-type: none"> • To view the check results of a specific compliance pack, click the security standard on the left. The check result details will be displayed on the right. • To search for a specific check item from a large number of check items, select a filter and press Enter. • To display certain columns only, click the setting button in the upper right corner of the check result list and complete the settings (for example, whether to wrap lines and whether to fix the operation column). • To view details about a check item, click the name of the check item to go to its details page. On the check item details page, view details about description, check process, check result, and checked resources.

----End

8.1.5 Handling Check Results

This section describes how to handle check results. You may need to carry out any of the following:

- **Handling Unsafe Settings:** Rectify the risky check items based on the check result.
- **Check Result Feedback:** For manual check items you performed offline, 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.
- **Importing Check Results:** Export the online check result to a local PC.
- **Exporting Check Results:** Import offline check results to the SecMaster baseline inspection page.

Limitations and Constraints

When you import check results, note the following restrictions:


- Only .xlsx files can be imported.
- Each time only one file can be imported. Maximum file size: 500 KB and 500 records.
- Duplicate data will be removed and will not be imported repeatedly.

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 part of the page and choose **Security > SecMaster**.

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

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

Step 5 In the check result list in the lower part of the check result page, click the name of the target check item to go to its details page.

Step 6 View the description of the check item and rectify the fault based on the suggestions in the **Recommendation** column


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

----End

Check Result Feedback

For manual check items you performed offline, report check results 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 part of the page and choose **Security > SecMaster**.

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

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

Step 5 In the check result list in the lower part of the **Check Result** tab, click **Manual Check** in the **Operation** column of the target check item.

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

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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.

Step 5 Click the name of the target compliance pack to go to its details page.

Step 6 Search for the target check item in the compliance pack list and click **Ignore** in the **Operation** column.

Step 7 In the displayed dialog box, click **OK**.


 **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 **Cancel Ignore** in the **Operation** column. Then, in the displayed dialog box, click **OK**.

----End

Importing Check Results

Step 1 Log in to the management console.

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

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

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

Step 5 In the upper left corner above the check result list, click **Import**.

Step 6 In the dialog box displayed, click **Download Template** and complete the template.

Step 7 In the displayed dialog box, click **Add File** and upload the completed template file.


 **NOTE**

- Only .xlsx files can be imported.
- Each time only one file can be imported. Maximum file size: 500 KB and 500 records.
- Duplicate data will be removed and will not be imported repeatedly.

Step 8 Click **Import**.

----End

Exporting Check Results

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.
- Step 5** Select the target compliance pack and click **Export** in the upper left corner above the compliance pack list.
- Step 6** In the displayed dialog box, select the format and data columns you want.
- Step 7** Click **OK**.

----End

8.1.6 Viewing Compliance Packs

This topic describes where to learn what compliance packs you have.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.
- Step 5** View details about compliance packs. For details about the parameters, see [Table 8-4](#).

Table 8-4 Parameters for compliance packs

Parameter	Description
Total Compliance Packs	Total number of existing compliance packs are organized, as well as the number of compliance packs by their statuses. The compliance pack status can be Enabled or Disabled .
Built-in Compliance Packs	The number of compliance packs preconfigured in SecMaster.
Custom Compliance Packs	The number of compliance packs you create.

Parameter	Description
<i>Compliance packs and their details</i>	<p>All compliance packs and their basic information.</p> <ul style="list-style-type: none"> • In the compliance pack list, you can view the type, status, and number of check items of a compliance pack. You can also enable, disable, and delete a compliance pack. • To search for a specific compliance, select a filter and press Enter. • To display certain columns only, click the setting button in the upper right corner of the compliance pack list and complete the settings (for example, whether to wrap lines and whether to fix the operation column). • To view details about a compliance pack, click its name to go to its details page. On the compliance pack details page, you can view its version, description, and check items.

----End

8.1.7 Creating a Custom Compliance Pack

This topic walks you through on how to create a custom compliance pack.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.
- Step 5** In the upper left corner above the compliance list, click **Add**
- Step 6** On the displayed page, configure basic information about the compliance pack.


Table 8-5 Basic information

Parameter	Description
Compliance Pack	The compliance pack name you specify.
Description	Description of the compliance pack.

Parameter		Description
(Optional) Advanced	Version	Set the compliance pack version.
	Classify	Enter the category the compliance pack belongs to.
	Domain	Enter the domain the compliance pack belongs to.
	Owner	The people in charge of the compliance pack.
	Applicable Region	Enter the region where the compliance pack is used.

Step 7 Click **Next** to go to the configuration page.

Step 8 On the displayed page, complete other parameters of the compliance pack.

1. In the navigation pane on the left, click . In the displayed text box, enter the node name and click **OK**.
 - Adding a subnode: To add a level-2 or level-3 node, hover over the node name and click the **Create** button. In the text box displayed, enter the node name and press **Enter**.
 - Editing or deleting a node: To edit or delete a node, hover over the node name and click the **Edit** or **Delete** button.
2. Select the name of an added node (minimum level. For example, if a level-3 node is added, select the level-3 node name). In all check items displayed on the right, select the check items you want to associate.

Step 9 Click **Next** to enter the confirmation page.

Step 10 Confirm the settings and click **OK**.

----End

Related Operations

- Disabling a compliance pack
 - a. In the row that contains the target compliance pack, click **Disable** in the **Operation** column.
 - b. In the displayed dialog box, click **OK**.
- Enabling a compliance pack
 - a. Click **Enable** in the **Operation** column of the compliance pack you want to enable.
 - b. In the displayed dialog box, click **OK**.
- Editing check items in a compliance pack
 - a. Click the name of the compliance pack you want to edit to go to its details page.
 - b. Click **Edit** in the **Compliance Pack Content** area.

- c. Edit check node information and their associated check items and click **OK**.
- Deleting a compliance pack
 - a. In the row that contains the compliance pack you want to delete, click **Delete** in the **Operation** column.
 - b. In the displayed dialog box, enter **DELETE** and click **OK**.

8.1.8 Importing and Exporting a Compliance Pack

Scenarios

This section describes how to import and export a compliance pack.


Limitations and Constraints

When you import a compliance pack, note the following restrictions:

- Only .xlsx files can be imported.
- Only one file can be imported at a time. Maximum file size: 100 records.

Importing a Compliance Pack

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.

Step 5 In the upper left corner above the compliance pack list, click **Import**.

Step 6 In the dialog box displayed, click **Download Template** and complete the template.

Step 7 In the displayed dialog box, click **Add File** and upload the completed template file.

NOTE


- Only .xlsx files can be imported.
- Only one file can be imported at a time. Maximum file size: 100 records.

Step 8 Click **Import**.

----End

Exporting a Compliance Pack

Step 1 Log in to the management console.

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

- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
 - Step 4** In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Compliance Pack** tab.
 - Step 5** Select the target compliance pack and click **Export** in the upper left corner of the compliance pack list.
 - Step 6** In the displayed dialog box, select the format and data columns you want.
 - Step 7** Click **Export**.
- End

8.1.9 Viewing Check Items

This section describes how to view existing check items.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Item** tab.
- Step 5** On the **Check Item** tab, view the information about existing check items. For details about the parameters, see [Table 8-6](#).

Table 8-6 Parameters for check items

Parameter	Description
Check Items	Total number of check items in the current workspace.
Built-in Check Items	The number of check items preconfigured in SecMaster.
Custom Check Items	The number of check items you create.

Parameter	Description
<i>Check items and details</i>	<p>All check items and their basic information.</p> <ul style="list-style-type: none"> • In the check item list, you can view the description, type, and number of compliance packs used for a check item. You can also edit or delete custom check items. • If there are a large number of check items, you can select a filter and press Enter to search for a specific resource. • To display certain columns only, click the setting button in the upper right corner of the check item list and complete the settings (for example, whether to wrap lines and whether to fix the operation column). • To view details about a check item, click its name. The details page is displayed on the right. On the check item details page, you can view the description and compliance pack used for the check item.

----End

8.1.10 Creating a Custom Check Item

This topic describes how to create a custom check item.

Limitations and Constraints

For custom check items, SecMaster does not check them immediately after they are created. You need to perform an immediate check manually or check the compliance pack the check items associated with. Then, you can get their check results.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Item** tab.
- Step 5** Click **Create Check Item** in the upper left corner of the check item list.
- Step 6** On the **Create Check Item** page, set check item parameters.

Table 8-7 Parameters for creating check items

Parameter	Description
Check Item	Name you specify for the check item.
Description	Description you provide for the check item.
Severity	Select the severity of the check item.
Action	Select an action for the check item. <ul style="list-style-type: none"> ● Executed by workflows: The check item is automatically executed through a workflow you specify, and the check result is reported by the workflow as well. ● Executed manually: You will manually complete the check item offline.
Select Workflow	If Action for a check item is set to Executed by workflows , you need to select a workflow for the check item. If no appropriate workflows are available, click Create Workflow and create one on the workflow page.
Manual Check Items	If Action for a check item is set to Executed manually , SecMaster sets the check result options by default.
Cloud service	Enter the information about the cloud service associated with the check item.

Step 7 Click **OK**.

 **NOTE**

For custom check items, SecMaster does not check them immediately after they are created. You need to perform an immediate check manually or check the compliance pack the check items associated with. Then, you can get their check results.

----End

Related Operations

- Editing check items in a compliance pack
 - a. In the row containing the target check item, click **Edit** in the **Operation** column.
 - b. On the **Edit Check Item** page, edit the check item parameters and click **OK**.
- Deleting a check item
 - a. In the row that contains the check item you want to delete, click **Delete** in the **Operation** column.
 - b. In the displayed dialog box, enter **DELETE** and click **OK**.

8.1.11 Importing and Exporting Check Items

Scenarios

This topic describes how to import and export check items.


Limitations and Constraints

When you import check items, note the following restrictions:

- Only .xlsx files can be imported.
- Only one file can be imported at a time. Maximum file size: 100 records.

Importing Check Items

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Item** tab.

Step 5 In the upper left corner above the check item list, click **Import**.

Step 6 In the dialog box displayed, click **Download Template** and complete the template.

Step 7 In the displayed dialog box, click **Add File** and upload the completed template file.

 **NOTE**


- Only .xlsx files can be imported.
- Only one file can be imported at a time. Maximum file size: 100 records.

Step 8 Click **OK**.

----End

Exporting Check Items

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Risk Prevention > Baseline Inspection**. On the displayed page, click the **Security Standards** tab. Then, click the **Check Item** tab.

Step 5 Select check items you want to export from the check item list and click **Export** in the upper left corner above the list.

Step 6 In the displayed dialog box, select the format and data columns you want.

Step 7 Click **Export**.

----End

8.2 Vulnerability Management

8.2.1 Overview

Background

SecMaster can integrate the vulnerabilities scanned by Host Security Service (HSS) and display them centrally. You can quickly locate vulnerable assets and fix vulnerabilities.

ECS Vulnerabilities

SecMaster can display vulnerabilities scanned by HSS in real time. You can view vulnerability details and find fixing suggestions.

The following host vulnerabilities can be detected:

Table 8-8 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.
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.

The vulnerability severity levels in SecMaster and vulnerability fix priorities in HSS are as follows:

- HSS: The vulnerability fix priority is weighted based on the CVSS score, release time, and the importance of the assets affected by the vulnerability. It reflects the urgency of the fix.

HSS classifies vulnerability fix priorities into four levels: critical, high, medium, and low. You can refer to the priorities to fix the vulnerabilities that have significant impact on your server first.

- SecMaster: The vulnerability severity is determined by CVSS scores. It reflects how severe the vulnerability is.

SecMaster classified vulnerability severity into four levels: high, medium, low, and informative. You can fix vulnerabilities based on their severity.

8.2.2 Viewing Vulnerability Details

Scenario

This topic describes how to view vulnerabilities details.

Prerequisites

- You have installed HSS agent. For details, see the *Host Security Service User Guide*.
- HSS logs have been connected to SecMaster and the function of automatically converting logs to alerts has been enabled. For details, see [Data Integration](#). If access to HSS vulnerability scan results has been enabled during data integration but the automatic alert conversion is disabled, the vulnerability scan results will not be displayed on the **Vulnerabilities** page in SecMaster.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Risk Prevention > Vulnerabilities**.
- Step 5** View vulnerability information on the **Vulnerabilities** page.

Table 8-9 Viewing vulnerability information

Parameter	Description
Vulnerability Type Distribution	This graph displays the total number of vulnerabilities and the distribution of vulnerabilities by type.

Parameter	Description
Top 5 Vulnerabilities	<ul style="list-style-type: none"> The Top 5 Vulnerabilities area lists the five vulnerabilities with the most affected assets. The more affected assets, the higher the vulnerability ranking is. The Vulnerability ID tab displays the IDs and the affected asset quantity for the five vulnerabilities. The Vulnerability Type tab displays the names, severity levels, and affected asset quantity for the five vulnerabilities.
Top 5 Vulnerable Resources	This graph displays the five resources with the most vulnerabilities.
<i>Vulnerability List</i>	<ul style="list-style-type: none"> The vulnerable list area includes Linux Vulnerabilities, Windows Vulnerabilities, Web-CMS Vulnerabilities, and Application Vulnerabilities tabs. Table 8-10 lists parameters for these vulnerability tabs. If there are many vulnerabilities displayed, use filters to search for a specific one. To view details about a vulnerability, click the vulnerability name and view the details on the page displayed on the right. You can view the total number of vulnerabilities below the vulnerability list. You can view a maximum of 10,000 vulnerability records page by page. To view more than 10,000 records, optimize the filter criteria.

Table 8-10 Vulnerability parameters

Parameter	Description
Vulnerability Name	Name of the scanned vulnerability. Click a vulnerability name to view vulnerability description and vulnerability library information.
Severity	Severity level of the vulnerability.
ID	ID of the vulnerability.
Affected Assets	Total number of assets affected by a vulnerability
Vulnerability ID	ID of a vulnerability.
Last Scanned	Time of the last scan
Handled	This column specifies whether the vulnerability has been handled.

----End

8.2.3 Fixing Vulnerabilities

Scenario

If HSS detects a vulnerability on a server, you need to handle the vulnerability in a timely manner based on its severity and your business conditions to prevent further vulnerability exploits.

If a vulnerability may harm your services, fix it as soon as possible. For Linux and Windows vulnerabilities, you can go to the HSS console and fix them in one-click. Web-CMS, emergency, and application vulnerabilities cannot be automatically fixed. You can handle them by referring to the suggestions provided on the vulnerability details page.

Constraints and Limitations

- For details about vulnerability management in Host Security Service (HSS) editions, see Host Security Service User Guide.
- To handle vulnerabilities on a server, ensure the server is in the **Running** state, its agent status is **Online**, and its protection status is **Protected**.


Precautions

- 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 prevent unexpected consequences, you are advised to use CBR to back up ECSs. 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 use external image sources to fix vulnerabilities.

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 part of the page and choose **Security > SecMaster**.

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

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

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.

To fix vulnerabilities in batches, select all the target vulnerabilities and click **Batch Repair** in the upper left corner above the list.

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

One-click automatic fix of Web-CMS or application vulnerabilities is not supported. You can log in to the server to manually fix them by referring to the fix suggestions on the vulnerability details slide-out panel.

- **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 8-11](#).

 **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 8-11 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.**

- Create an image for the ECS host whose vulnerability needs 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 8-12 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.

8.2.4 Importing and Exporting Vulnerabilities

Scenario

This section describes how to import and export vulnerabilities.


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

Constraints

- Only .xlsx files no larger than 5 MB can be imported.
- A maximum of 9,999 vulnerability records can be exported from SecMaster.

Importing Vulnerabilities

Step 1 Log in to the management console.

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

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

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

Step 5 On the displayed page, select a tab to go to the corresponding vulnerability management page.

For example, to import Linux vulnerabilities, click the **Linux Vulnerabilities** tab.

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.

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

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 part of the page and choose **Security > SecMaster**.

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

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

Step 5 On the **Vulnerabilities** page, click the target vulnerability tab.

For example, if you want to export Linux vulnerabilities, click the **Linux Vulnerabilities** tab.

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 8-13 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

8.2.5 Ignoring and Unignoring a Vulnerability


Scenario

Some vulnerabilities are risky only in specific conditions. For example, if a vulnerability can be exploited only through an open port, but there are no open ports on the target server, the vulnerability will not harm the server. Such vulnerabilities can be ignored. HSS will still generate alerts when next time it finds the vulnerabilities you ignore before. SecMaster will synchronize the vulnerability information as well. You can also unignore a vulnerability as needed.

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 part of the page and choose **Security > SecMaster**.

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

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

Step 5 On the **Vulnerabilities** page, click any vulnerability type tab. In the vulnerability list, click the name of the target vulnerability. The vulnerability details page is displayed on the right.

For example, if you want to handle a Linux vulnerability, click the **Linux Vulnerabilities** tab and click the target vulnerability name. Then, you can view the vulnerability details on the page displayed on the right.

Step 6 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

8.3 Policy Management

8.3.1 Overview

SecMaster provides policy management for you to manage and maintain tasks across accounts and resources. With this function, you can view all policies centrally, manage policies for seven defense lines manually, and query manual and automatic block records quickly.

Limitations and Constraints

- Currently, the emergency policies include only the WAF blacklist policies and VPC security groups.
- A maximum of 300 emergency policies that support block aging can be added for a single workspace you have. A maximum of 1,300 emergency policies can be added for a single workspace you have. Limits on blocked objects at a time are as follows:
 - When a policy needs to be delivered to WAF, each time a maximum of 50 IP addresses can be added as blocked objects for each account.
 - When a policy needs to be delivered to VPC, each time a maximum of 20 IP addresses can be added as blocked objects within 1 minute for each account.
- If an IP address is added to the blacklist, VPC or WAF will block requests from that IP address without checking whether the requests are malicious.

8.3.2 Adding and Editing an Emergency Policy

Scenario

An emergency policy is used to quickly block attacks. You can select a block type based on the alert source to block attackers.

This topic describes how to add and edit an emergency policy.


Limitations and Constraints

- A maximum of 300 emergency policies that support block aging can be added for a single workspace you have. A maximum of 1,300 emergency policies can be added for a single workspace you have. Limits on blocked objects at a time are as follows:
 - When a policy needs to be delivered to WAF, each time a maximum of 50 IP addresses can be added as blocked objects for each account.

- When a policy needs to be delivered to VPC, each time a maximum of 20 IP addresses can be added as blocked objects within 1 minute for each account.
- If an IP address is added to the blacklist, VPC or WAF will block requests from that IP address without checking whether the requests are malicious.
- Once an emergency policy is added, its blocked object type and blocked objects, such as IP addresses and IP address ranges, cannot be modified.

Adding an Emergency Policy

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Risk Prevention > Security Policies**. Then, go to the emergency policy page.

Step 5 On the **Emergency Policies** page, click **Add**. The page for adding policies slides out from the right of the page.

Step 6 On the **Add** page, configure policy information.

Table 8-14 Emergency policy parameters

Parameter	Description
Blocked Object Type	Type of the object you want to block. You can select IP .
Block Object	<ul style="list-style-type: none"> • If you select IP for Blocked Object Type, enter one or more IP addresses or IP address ranges you want to block. If there are multiple IP addresses or IP address ranges, separate them with commas (,). • There are some restrictions on delivery of blocked objects: <ul style="list-style-type: none"> - When a policy needs to be delivered to WAF, each time a maximum of 50 IP addresses can be added as blocked objects for each account. - When a policy needs to be delivered to VPC, each time a maximum of 20 IP addresses can be added as blocked objects within 1 minute for each account.
Label	Label of a custom emergency policy.
Operation Connection	Asset connections that are used to operate blocking workflows of security services in the seven layers of defense. Select the operation connection for the policy.

Parameter	Description
Block Aging	<p>Check whether the policy needs to be stopped.</p> <ul style="list-style-type: none"> If you select Yes, set the aging time of the policy. For example, if you set the aging time to 180 days, the policy is valid within 180 days after the setting. After 180 days, the IP address/range will not be blocked. If you select No, the policy is always valid and blocks the specified IP address/range.
Policy Description	Description of the custom policy.

Step 7 Click **OK**.


----End

Editing an Emergency Policy

NOTE

Once an emergency policy is added, its blocked object type and blocked objects, such as IP addresses and IP address ranges, cannot be modified.

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Risk Prevention > Security Policies**. Then, go to the emergency policy page.

Step 5 On the emergency policy management page, locate the row that contains the policy you want to edit and click **Edit** in the **Operation** column.

Step 6 On the edit policy page, modify the policy information.

Table 8-15 Editing an emergency policy

Parameter	Description
Blocked Object Type	After an emergency policy is added, its blocked object cannot be modified.
Blocked Object	After an emergency policy is added, its blocked object cannot be modified.
Label	Label of a custom emergency policy.
Operation Connection	Select the operation connection for the policy.

Parameter	Description
Block Aging	<p>Check whether the policy needs to be stopped.</p> <ul style="list-style-type: none"> If you select Yes, set the aging time of the policy. For example, if you set the aging time to 180 days, the policy is valid within 180 days after the setting. After 180 days, the IP address/range will not be blocked. If you select No, the policy is always valid and blocks the specified IP address/range.
Policy Description	Description of the custom policy.

Step 7 Click **OK**.

----End


8.3.3 Viewing Emergency Policies

Scenario

This section describes how to view emergency policies.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Risk Prevention > Security Policies**. Then, go to the emergency policy page.

Step 5 In the upper part of the emergency policy page, view emergency policy statistics.

- Number of delivered policies: collects statistics on the number of policies delivered to each cloud product.
- Top 3 Operation Connections: displays statistics on top 3 operation connections blocked by policies and the number of blocked operation connections.
- Top 5 Blocking Areas: displays top 5 blocked areas and their distribution.

Step 6 In the policy list, view the information about the emergency policy. The parameters are as follows.

Table 8-16 Emergency policy parameters

Parameter	Description
Block Object	IP addresses or IP address ranges to be blocked.

Parameter	Description
Label	Label information of the policy.
Number of delivered policies	Number of policies delivered to corresponding product.
Block Type	Block type configured for the policy.
Creator	Creator of the policy.
Reason Description	Policy description.
Creation Time	Time when the policy was created.
Operation	You can edit or delete a policy.

Step 7 To view details about an emergency policy, select the policy and click **Selected: xxx** in the lower part of the page to open the details page.

On the details page, you can block, cancel blocking, and delete a policy, and view historical records of the policy.

----End


8.3.4 Deleting an Emergency Policy

Scenario

This section describes how to delete emergency policies or delete emergency policies in batches.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Risk Prevention > Security Policies**. Then, go to the emergency policy page.

Step 5 On the emergency policy page, locate the row that contains the policy you want to delete and click **Delete** in the **Operation** column.

To delete multiple policies, select the target policies and click **Batch Delete** above the list.

Step 6 In the displayed confirmation dialog box, click **Confirm**.

----End

8.3.5 Blocking or Canceling Blocking of an IP Address or IP Address Range

Scenario


If an IP address or IP address range added as blocked object for an emergency policy needs to be blocked in other operation connections, you can block them in batches. If there is no need to block an IP address or IP address range for operation connections, you can cancel the blocking in batches.

This section describes how to block or cancel blocking of IP addresses or IP address ranges in multiple connections.

Limitations and Constraints


If an IP address is added to the blacklist, VPC will block requests from that IP address without checking whether the requests are malicious.

Enabling an IP Address Blocklist for Multiple Connections

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Risk Prevention > Security Policies**. Then, go to the emergency policy page.
- Step 5** On the emergency policy page, locate the row that contains the policy you want to enable batch block and click **Batch Block** in the **Operation** column.
- Step 6** In the displayed dialog box, enter the blocking reason and click **OK**.

----End

Canceling Batch Block

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Risk Prevention > Security Policies**. Then, go to the emergency policy page.
- Step 5** On the emergency policy page, locate the row that contains the target policy, click **Cancel Blocking in Batches** in the **Operation** column.

Step 6 In the dialog box displayed, enter the reason for canceling the blocking and click **OK**.

----End

9 Threat Operations

9.1 Incident Management

9.1.1 Viewing Incidents

Scenario

An incident is a broad concept. It can include but is not limited to alerts. It can be a part of normal system operations, exceptions, or errors. In the O&M and security fields, an incident usually refers to a problem or fault that has occurred and needs to be focused on, investigated, and handled. An incident may be triggered by one or more alerts or other factors, such as user operations and system logs.

An incident is usually used to record and report historical activities in a system for analysis and audits.

On the **Incidents** page in SecMaster, you can check the incident list for the last 360 days. The list contains incident names, types, severity levels, 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Incidents**.
- Step 5** On the **Incidents** page, view incident details.

Figure 9-1 Viewing incidents

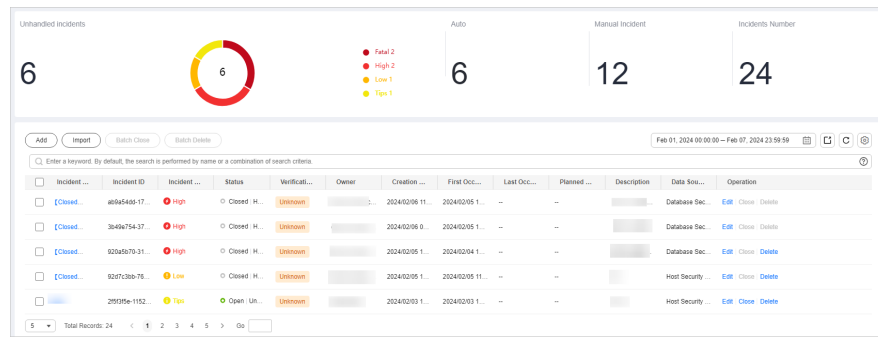


Table 9-1 Viewing an Incident

Parameter	Description
Unhandled Incidents	This area displays how many incidents that are not handled within the specified time range in the current workspace. The unhandled incidents are displayed by severity.
Auto (Incidents Handled Automatically)	This area displays how many incidents that are handled automatically by playbooks within the specified time range in the current workspace.
Manual Incident (Incidents Handled Manually)	This area displays how many incidents that are handled manually within the specified time range in the current workspace.
Incidents Number (Incidents)	This area displays how many incidents that are reported within the specified time range in the current workspace.

Parameter	Description
Incident list	<p>The list displays more details about each incident. You can view the total number of incidents below the incident list. You can view a maximum of 10,000 incident records page by page. To view more than 10,000 records, optimize the filter criteria.</p> <p>In the incident list, you can view the incident name, severity, source, and status. To obtain overview of an incident, click the incident name. The incident overview panel is displayed on the right.</p> <ul style="list-style-type: none"> • On the Incident Overview panel, you can view incident handling suggestions, basic information, and associated information (including associated threat indicators, alerts, incidents, and attack information). • To view incident details, click Incident Details in the lower right corner of the incident overview panel. The incident details page is displayed. On the details page, you can view the incident timeline and attack information in addition to the information on the overview page. For example, you can view the first occurrence time of an incident, detection time, and attack process ID. • On the incident overview or details page, you can change the incident severity and status in the corresponding drop-down list boxes. • On the incident overview or details page, you can associate or disassociate alerts, incidents, and indicators and view information about affected resources.

----End


9.1.2 Adding and Editing an Incident

Scenario

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 part of the page and choose **Security > SecMaster**.

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

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

Step 5 On the **Incidents** page, click **Add**. On the displayed **Add** page, set parameters as described in [Table 9-2](#).

Table 9-2 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
	Type	Incident type
	(Optional) Service ID	Enter the service ID corresponding to the incident.
	Incident Severity	Select a severity level.
	Status	Select an incident status.
	(Optional) Owner	Primary owner of the incident.
	Data Source Product Name	Select the name of the data source product.
	Data Source Type	Select the type of the data source. For example, if the data source is a cloud service, select the cloud service.
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.


Parameter		Description
	(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. ● Containment, extradition, and recovery: Handle an incident. ● Post Incident Activity: Follow-up activities.
	(Optional) Debugging data	Whether to enable simulated debugging
	(Optional) Labels	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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Threat Operations > 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 9-3 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

Parameter		Description
	Incident Type	Incident type
	(Optional) Service ID	Enter the service ID corresponding to the incident.
	Incident Level	Select a severity level.
	Status	Select an incident status.
	(Optional) Owner	Primary owner of the incident.
	Data Source Name	Name of the data source, which cannot be changed
	Data Source Type	Type of the data source, which cannot be changed
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.
	(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

9.1.3 Importing and Exporting Incidents

Scenario


This section describes how to import and export incidents.

Limitations and Constraints

- Only .xlsx files no larger than 5 MB can be imported.
- A maximum of 9,999 incident records can be exported.

Importing Incidents

Step 1 Log in to the management console.

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

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

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

Step 8 Click **OK**.

----End


Exporting Incidents

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Threat Operations > 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 9-4 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


9.1.4 Closing or Deleting Incidents

Scenario

This topic describes how to close and delete an incident.

Procedure

Step 1 Log in to the management console.

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

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

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

Step 5 On the **Incidents** page, close or delete an incident.

Table 9-5 Managing incidents

Operation	Description
Closing an Incident	<ol style="list-style-type: none"> 1. Locate the row that contains the target incident and click Close in the Operation column. To close multiple incidents, select them in the incident list and click Close above the list. 2. In the confirmation dialog box, select Reason for, enter Close Comment, and click OK.
Deleting an Incident	<ol style="list-style-type: none"> 1. On the Incident page, locate the row that contains the target incident and click Delete in the Operation column. To delete multiple incidents, select the target incidents in the incident list and click Delete above the list. 2. In the dialog box that is displayed, click OK. <p>NOTE Deleted incidents cannot be restored. Exercise caution when deleting an incident.</p>

----End

9.2 Alert Management

9.2.1 Viewing Alerts

Scenario

An alert is a notification of abnormal signals in O&M. It is usually automatically generated by a monitoring system or security device when detecting an exception in the system or networks. For example, when the CPU usage of the server exceeds 90%, the system may generate an alert. These exceptions may include system faults, security threats, or performance bottlenecks.

Generally, an alert can clearly indicate the location, type, and impact of an exception. In addition, alerts can be classified by severity, such as critical, major, and minor, so that O&M personnel can determine which alerts need to be handled first based on their severity.

The purpose of an alert is to notify related personnel in a timely manner so that they can make a quick response and take measures to fix the problem.

When SecMaster detects an exception (for example, a malicious IP address attacks an asset or an asset has been hacked into) in cloud resources, it generates an alert and displays the threat information on the **Alerts** page in SecMaster.


On the **Alerts** page in SecMaster, you can check the alert list for the last 360 days. The list contains alert names, types, severity levels, and occurrence 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.

Prerequisites

To check alerts from other cloud services, you need to enable the function of automatically converting logs to alerts on the **Data Integration** page. If this function is disabled, logs that meet certain alert rules will not be converted to alerts or displayed on the **Alerts** page. For details, see [Enabling Log Access](#).

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Alerts**.

Step 5 View alert information.

Table 9-6 Viewing Alerts

Parameter	Description
Time ranges (Today , This week , This month , or Customize)	In the upper right corner on the page, you can select a time range to view alerts generated during this period. By default, alerts generated in the current week are displayed.
Unhandled Alerts	This area displays how many alerts that are not handled within the specified time range in the current workspace. The unhandled alerts are displayed by severity.
Alerts Handled Automatically (Auto)	This area displays how many alerts that are handled automatically by playbooks within the specified time range in the current workspace.
Alerts Handled Manually (Manual)	This area displays how many alerts that are handled manually within the specified time range in the current workspace.
Alerts	This area displays how many alerts that are reported within the specified time range in the current workspace.

Parameter	Description
Alarm list	<p>The list displays more details about each alert.</p> <p>You can view the total number of alerts below the alert list. You can view a maximum of 10,000 alert records page by page. To view more than 10,000 records, optimize the filter criteria.</p> <p>In the alert list, you can view the alert type, summary, severity, source, and handling status. To view details about an alert, click its name. On the alert details page displayed:</p> <ul style="list-style-type: none"> • You can comment on, block, unblock, close, and delete the alert, convert the alert to an incident, and refresh the alert status. • You can view the security overview, context, relationship, and comments about the alert. <ul style="list-style-type: none"> - Security Overview: On this tab, you can view the summary, handling suggestions, basic information, and request details of the alert. - Context: On this tab, you can view the key and full context information of the alert in JSON format or in a table. - Relationship: On this tab, you can view associated information, such as associated alerts, incidents, indicator, and affected assets, about the alert. - Comment: On this tab, you can view historical comments on the alert and make your comments.

----End

9.2.2 Converting an Alert to an Incident or Associating an Alert with an Incident

Scenario

SecMaster analyzes alerts it aggregates from other services. During the analysis, if SecMaster detects attacks or serious threats, it converts such alerts into incidents or associates such alerts with certain incidents.

This section describes how to convert an alert to an incident and how to associate an alert with an incident.

Relationships Between Alerts and Incidents

This part describes the meanings and differences between alerts and incidents, reasons for converting alerts to incidents, and reasons for associating alerts with incidents.

- **Meanings and Differences Between Alerts and Incidents**

Table 9-7 Meanings and differences between alerts and incidents

Type	Description
Definition	<ul style="list-style-type: none"> • Alerts An alert is a notification of abnormal signals in O&M. It is usually automatically generated by a monitoring system or security device when detecting an exception in the system or networks. For example, when the CPU usage of the server exceeds 90%, the system may generate an alert. These exceptions may include system faults, security threats, or performance bottlenecks. Generally, an alert can clearly indicate the location, type, and impact of an exception. In addition, alerts can be classified by severity, such as critical, major, and minor, so that O&M personnel can determine which alerts need to be handled first based on their severity. The purpose of an alert is to notify related personnel in a timely manner so that they can make a quick response and take measures to fix the problem. • Incidents An incident is a broad concept, and may include, but is not limited to, an alert. An incident can be a part of the normal operation of the system, an exception, or an error. In the O&M and security fields, an incident usually refers to a problem or fault that has occurred and needs to be focused on, investigated, and handled. An incident may be triggered by one or more alerts or other factors, such as user operations and system logs. An incident is usually used to record and report historical activities in a system for analysis and audits.

Type	Description
Handling process	<ul style="list-style-type: none"> ● Alerts The alert handling process includes receiving, confirming, analyzing, responding to, and closing alerts. When the monitoring system generates an alert, O&M personnel need to confirm that the alert is a positive one. Then, they need to analyze the alert causes and impact scope, take measures to rectify the fault, and close the alert. ● Incidents The event handling process is more complex and comprehensive. In addition to each phase in the alert handling process, incident handling also involves incident investigation, impact assessment, risk analysis, emergency plan formulation, emergency response execution, and post-event summary. The objective of incident handling is to completely solve problems, prevent similar incidents in the future, and reduce the impact of incidents on services.
Importance and urgency	<ul style="list-style-type: none"> ● Alerts Generally, alerts need to be evaluated and responded immediately. The severity and importance of each alert vary depending on the alert type, severity, and impact scope. Some alerts may be simple reminders or warnings, while others may indicate that the system has been severely attacked or faces major fault risks. ● Incidents In some cases, incidents may need to be recorded, analyzed, and handled, but do not require immediate responses. An incident is usually of higher importance and urgency than an alert. Because an incident has occurred and has had an actual impact, immediate measures need to be taken to control the risk and solve the problem. If an incident is not handled in a timely manner, it may cause significant economic loss or reputation damage to the organization.

- **Causes for converting alerts to incidents or associating alerts with incidents**

An alert is a notification generated when a system or service becomes abnormal or a potential fault occurs. These exceptions may directly affect service availability. So alerts must be handled in a timely manner to prevent service exceptions. When an alert is generated, you need to take corresponding measures to rectify the fault. Otherwise, services may be abnormal due to these exceptions or faults.

An incident is a notification generated when the system or service is running properly. An event may involve some important status changes, but may not

cause service exceptions. So incidents do not need to be handled. They are mainly used to analyze and locate problems.

Table 9-8 Causes for converting alerts to incidents or associating alerts with incidents

Type	Description
<p>Alert-to-Incident reasons</p>	<p>When the severity of an alert reaches a certain level, an alert appears continuously, or the impact scope is wide, the alert may not only be a signal that requires attention. It also indicates that a continuous problem exists in the system or network. In this case, the alert has evolved into an incident that needs to be handled immediately. So, we need to convert such alerts to incidents to further investigate the root causes and take necessary measures. Generally, an alert will be converted to an incident out of the following causes:</p> <ul style="list-style-type: none"> ● Information aggregation and classification An alert is usually an instant response to a violation against a specific condition or threshold. The number of alerts is increasing over time. If they are handled independently, it would cause chaos and waste time and human resources. Aggregating these alerts into incidents helps related personnel classify alerts by alert type, source, and impact so that they can handle them more effectively. ● Simplified working processes During the process to convert alerts to incidents, alerts are filtered, deduplicated, and aggregated. So that multiple similar alerts that may be triggered are integrated into a more representative incident. In this way, the workload of handling alerts is reduced; the handling process is clearer; and the tracing and recording become easier. ● Higher problem-solving efficiency As an incident has much more context details than an alert, related personnel can easily identify the root cause. This helps quickly locate issues and take effective measures. ● Historical data review and trend analysis An incident usually records the entire process of how an issue occurred, evolved, and is resolved. So converting alerts to incidents provides helpful historical data for prevention of similar issues and system optimization. By analyzing the trend of an incident, O&M personnel can discover potential weak points in the system and take measures in advance. ● Cross-department collaboration enhanced In a large organization, different departments may need to participate in the handling of problems. After an alert is converted to an incident, related information can be shared among departments more easily, which promotes cross-department


Type	Description
	<p>collaboration and improves problem solving efficiency.</p> <p>In a word, converting alerts to incidents helps simplify working processes, improve problem solving efficiency, and facilitate historical review and trend analysis.</p>

Type	Description
<p>Causes for associating alerts with incidents</p>	<p>As an important part of monitoring and fault management, associating alerts with incidents involve combining multiple independent but possibly correlated incidents or alerts to better understand the root cause and scope of a problem, facilitating troubleshooting and response. Generally, an alert will be associated with an incident out of the following causes:</p> <ul style="list-style-type: none"> • Dependencies In a complex system, there are complex dependencies between components. When a component becomes faulty, other components that depend on the component may be affected, causing a series of alerts. For example, in the microservice architecture, the crash of a service may cause problems in other services that use the service. • Resource sharing When multiple systems or services share the same resource (such as a server, database, or network device), the problem of the resource may cause multiple systems or services to generate alerts at the same time. For example, a performance deterioration of a shared database server may trigger performance alerts for multiple applications that depend on the database. • Chain reactions In some cases, an initial failure may trigger a series of chain reactions, affecting more components or systems. This chain reaction may be caused by improper system design, incomplete error handling mechanism, or resource limitations (such as performance deterioration caused by memory leakage). • Configuration errors Incorrect or inconsistent configurations may cause system behavior exceptions, triggering multiple seemingly irrelevant alerts. For example, incorrect routing configurations may cause traffic to be incorrectly routed to unstable servers, causing multiple performance-related alerts. • Software defects Software defects, such as bugs, may cause programs to be abnormal in specific conditions and trigger alerts. If these defects affect multiple components or systems, multiple associated alerts may be generated. • External factors External factors, such as natural disasters (such as earthquakes and floods), network attacks, and

Type	Description
	infrastructure faults (such as power outages and network interruptions), may also cause problems in multiple systems or components at the same time and trigger a large number of alerts.

Converting an Alert to an Incident

Step 1 Log in to the management console.

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

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

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

In addition, you can click **Alert-to-Incident** in the upper right corner of the details page of an alarm.

Step 6 On the **Convert to Incident** page, specify **Incident Name** and **Incident Type**.


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

Step 7 Click **OK**.

----End

Associating an Alert with an Incident

Step 1 Log in to the management console.

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

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

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

Step 5 In the alert list, select the alerts you want to associate and click **Associated Event** above the list. The **Bind Incident** dialog box is displayed.

Step 6 In the dialog box displayed, select the target incidents and click **OK**.

After the association is complete, click the type of the target alert in the alert list. On the alert details page displayed, choose **Relationship > Associated Incidents** and check the association details.

----End

9.2.3 Adding and Editing an Alert

Scenario

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Alerts**.
- Step 5** On the **Alerts** page, click **Add**. On the **Add** page displayed on the right, set parameters as described in [Table 9-9](#).

Table 9-9 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 Informational , Low , Medium , High , and Critical .
	Status	Alert status. The options are Open , Blocked , and Closed .
	(Optional) Owner	Primary owner of the alert.
	Data Source Product Name	Data source name
	Data Source Type	Type of the data source. The options are Cloud Service , Third-party , and Private .
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.


Parameter		Description
Other	(Optional) Verification Status	Verification status of the alert to identify the accuracy of the alert. 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. ● Containment, extradition, and recovery: Handle an alert. ● Post Incident Activity: Follow-up activities.
	(Optional) Debugging data	Whether to enable simulated debugging.
	(Optional) Labels	Alert labels.
	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 part of the page and choose **Security > SecMaster**.

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

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

Step 5 In the alert list, locate the row that contains the target alert and click **More > 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 9-10](#).

Table 9-10 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
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 alert. 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.

Parameter		Description
	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

9.2.4 Importing and Exporting Alerts

Scenario


This section describes how to import and export alerts.

Limitations and Constraints

- Only .xlsx files no larger than 5 MB can be imported.
- A maximum of 9,999 alert records can be exported.

Importing Alerts

Step 1 Log in to the management console.

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

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

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

Step 5 On the **Alerts** page, click **More > 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.

Step 8 Click **OK**.

----End

Exporting Alerts

Step 1 Log in to the management console.

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

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

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

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

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

Table 9-11 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


9.2.5 Closing or Deleting an Alert

Scenario

This topic describes how to close and delete an alert.

Procedure

Step 1 Log in to the management console.

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

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

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

Step 5 On the **Alerts** page, close or delete an alert.

Table 9-12 Managing alerts

Operation	Description
Closing an alert	<ol style="list-style-type: none"> 1. Locate the row that contains the target alert, click Close in the Operation column. A dialog box is displayed for you to confirm the close operation. To close multiple alerts, select the alerts in the alert list and click Batch Close above the list. 2. In the confirmation dialog box, select Reason for, enter Close Comment, and click OK.

Operation	Description
Deleting an alert	<p>1. Locate the row that contains the target alert, click More in the Operation column, and select Delete. The deletion confirmation dialog box is displayed. To delete multiple alerts, select the alerts in the alert list and click More > Batch Delete above the list.</p> <p>2. In the displayed dialog box, click OK.</p> <p>NOTE Deleted alerts cannot be restored. Exercise caution when deleting an alert.</p>

----End

9.2.6 One-click Blocking or Unblocking


Scenario

An emergency policy is used to quickly prevent attacks. You can select a block type based on the alert source to block attackers.

This topic describes how to block or unblock attack sources quickly.

One-click Blocking

Step 1 Log in to the management console.

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

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

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

Step 5 In the alert list, locate the row that contains the target alert and choose **Operation > One-Click Block** in the **Operation** column. The **One-Click Block** panel is displayed on the right.

You can also go to the details page of the target alert and click **One-Click Block** in the upper right corner of the page.

Step 6 On the displayed page, configure the blocking policy.

Table 9-13 One-click blocking


Parameter	Description
Block Object	<ul style="list-style-type: none"> If you select IP for Blocked Object Type, enter one or more IP addresses or IP address ranges you want to block. If there are multiple IP addresses or IP address ranges, separate them with commas (,). There are some restrictions on delivery of blocked objects: <ul style="list-style-type: none"> When a policy needs to be delivered to WAF, each time a maximum of 50 IP addresses can be added as blocked objects for each account. When a policy needs to be delivered to VPC, each time a maximum of 20 IP addresses can be added as blocked objects within 1 minute for each account.
Label	Label of the custom emergency policy.
Operation Connection	Select the operation connections for the policy.
Block Aging	<p>Check whether the policy needs to be stopped.</p> <ul style="list-style-type: none"> If you select Yes, set the aging time of the policy. For example, if you set the aging time to 180 days, the policy is valid within 180 days after the setting. After 180 days, the IP address or IP address range will not be blocked. If you select No, the policy is always valid and blocks the specified IP address or IP address range.
Policy Description	Description of the custom policy.

Step 7 Confirm settings and click **OK**. In the displayed dialog box, click **OK**.

----End

One-click Unblocking

Step 1 Log in to the management console.

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

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

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

Step 5 In the alert list, locate the row that contains the target alert, click **Operation > One-Click Unblock** in the **Operation** column.

You can also go to the details page of the target alert and click **One-Click Unblock** in the upper right corner of the page.

- Step 6** In the displayed dialog box, enter the reason and click **OK**.
----End

9.3 Indicator Management

9.3.1 Adding and Editing an Indicator

Scenario

The indicator library list displays information about all your indicators.

This section describes how to create and edit an indicator.

Adding an Indicator


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Indicators**.
- Step 5** On the **Indicators** page, click **Add**. On the **Add** page, set parameters.

Table 9-14 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. The options are Cloud Service , Third-party , and Private .
Status	Indicator status. Possible values are Open , Closed , and Revoked .


Parameter	Description
(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 .
Granularity	Granularity of the indicator. The options are First time observed, In-house data, To be purchased, and Queried from external networks .
<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

Editing an Indicator

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Threat Operations > 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 9-15 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	Name of the data source, which cannot be changed
Data Source Type	Type of the data source, which cannot be changed
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 , In-house data , To be purchased , and Queried from external networks .
<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 7 Click **OK**.

----**End**

9.3.2 Disabling and Deleting an Indicator

Scenario

This topic describes how to disable or delete an indicator.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Indicators**.
- Step 5** On the **Indicators** page, close or delete an indicator.

Table 9-16 Indicator parameters

Operation	Description
Close	<ol style="list-style-type: none"> On the Indicator page, locate the row that contains the target indicator, click Close in the Operation column. The Close dialog box is displayed. In the dialog box that is displayed, select the close reason and enter comments. Click OK.
Delete	<ol style="list-style-type: none"> On the Indicators page, locate the target indicator and click Delete in the Operation column. In the dialog box displayed, click OK. <p>NOTE Deleted indicators cannot be restored. Exercise caution when performing this operation.</p>

----End

9.3.3 Importing and Exporting Intelligence Indicators


Scenario

This section describes how to import and export intelligence indicators.

Constraints

- Only .xlsx files no larger than 5 MB can be imported.
- A maximum of 9,999 indicator records can be exported.

Importing an Indicator

- Step 1** Log in to the management console.
 - Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
 - Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
 - Step 4** In the navigation pane on the left, choose **Threat Operations > 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.
 - Step 8** Click **OK**.
- End

Exporting Indicators



- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > 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 9-17 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

9.3.4 Viewing Indicators

Scenario

This topic describes where to view existing intelligence indicators.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Indicators**.
- Step 5** On the **Indicators** page, view details about the indicator.

Table 9-18 Indicator parameters

Parameter	Description
Indicator Type	Indicator Type displays the total number of indicators of all types and the number of indicators of the corresponding type.
Overdue Indicator	Overdue Indicator displays the total number of threat indicators that have expired and have not been closed.
Indicator Status	Indicator Status displays the total number of indicators in different states and the number of indicators in the corresponding state.
Threat Degree	Threat Degree displays the number of indicators of different threat levels.
Indicator list	<p>Displays detailed information about each indicator. You can view the total number of indicators below the indicator list. You can view a maximum of 10,000 indicator records page by page. To view more than 10,000 records, optimize the filter criteria.</p> <p>You can view the threat degree, discovery time, and status of indicators. To view details about an indicator, click the indicator name. The indicator details are displayed on the right of the page.</p> <ul style="list-style-type: none"> ● On the Indicator Overview page, you can view basic information of an indicator as well as its association information, such as associated indicators, alerts, and incidents. ● In the Associated Information area, you can bind or unbind an indicator to or from other indicators, alerts, and incidents.

----End

9.4 Intelligent Modeling

9.4.1 Viewing Available Model Templates

Scenario

SecMaster uses models to scan log data in pipelines. If SecMaster detects data that hits the trigger in a model, SecMaster generates an alert. Models are created based on templates. Therefore, you need to use available templates to create models.

This section describes how to view available model templates.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Intelligent Modeling**, and select the **Model Templates** tab.
- Step 5** On the **Model Templates** tab, view available model templates.

Table 9-19 Template information

Parameter	Description
Model Template Statistics	This area displays how many Available templates and how many Active templates you have.
Severity	This bar displays the number of available templates by severity levels, including Critical, High, Medium, Low, and Informative .
Template list	<ul style="list-style-type: none"> • The template list displays the severity, name, and model type of each template as well as when the template is created and upgraded. • 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

9.4.2 Creating and Editing a Model

Scenario


SecMaster can use models to monitor log data in pipelines. If SecMaster detects the data that hits trigger conditions in a mode, SecMaster generates an alert.

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

- [Creating an Alert Model Using a Template](#)
- [Creating a Custom Alert Model](#)
- [Editing a Model](#)

Creating an Alert Model Using a Template

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Threat Operations > Intelligent Modeling**, and select the **Model Templates** tab.

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.

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 **Create Threat Model** page, configure basic information about the model by referring to [Table 9-20](#).

Table 9-20 Basic alert model parameters

Parameter	Description
Pipeline Name	Select the execution pipeline for the alert model based on the pipeline described in Restrictions area in the Description text box.
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.

Parameter	Description
Model Type	The default value is Rule model .
Description	Description of the alert model
Status	Indicates whether to enable the alert model. The status set here can be changed after the entire alert model is set successfully.

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 9-21](#).

Table 9-21 Configure Model Logic

Parameter	Description
Query Rule	<p>Set alert query rules. After the setting is complete, click Run and view the running result.</p> <p>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 Statements - SQL Syntax.</p> <p>NOTE If the reserved field is of the text type, MATCH_QUERY is used for word segmentation queries by default.</p>
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.

Parameter	Description
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 trigger conditions, click Add and add them. A maximum of five trigger conditions can be added.</p> <p>If there are multiple trigger conditions, SecMaster scans log data to hit each trigger condition from top to bottom and generates all types of alerts for hit trigger conditions.</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"> ● If Suppression is enabled, the query stops after an alert is generated. ● If Suppression is disabled, 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

Creating a Custom Alert Model

Step 1 Log in to the management console.

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

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

- Step 4** In the navigation pane on the left, choose **Threat Operations > Intelligent Modeling**.
- 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 9-22](#).

Table 9-22 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	Indicates whether to enable the alert model. The status set here can be changed after the entire alert model is set successfully.

- 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 9-23](#).

Table 9-23 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 Query and Analysis Statements - SQL Syntax .

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"> 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	<p>Setting alert triggering conditions. The value can be greater than, equal to, not equal to, or less than xx.</p> <p>To configure multiple trigger conditions, click Add and add them one by one. A maximum of five trigger conditions can be added.</p> <p>If there are multiple trigger conditions, SecMaster scans log data to hit each trigger condition and generates all types of alerts for hit trigger conditions.</p>
Alarm Trigger	<p>The way to trigger alerts for queried result. 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"> If Suppression is enabled, the query stops after an alert is generated. If Suppression is disabled, 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 part of the page and choose **Security > SecMaster**.

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

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

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 9-24](#).

Table 9-24 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 9-25](#).

Table 9-25 Configure Model Logic

Parameter	Description
Query Rule	<p>Set alert query rules. After the setting is complete, click Run and view the running result.</p> <p>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 Statements - SQL Syntax.</p> <p>NOTE If the reserved field is of the text type, MATCH_QUERY is used for word segmentation queries by default.</p>
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 trigger conditions, click Add and add them. A maximum of five trigger conditions can be added.</p> <p>If there are multiple trigger conditions, SecMaster scans log data to hit each trigger condition from top to bottom and generates all types of alerts for hit trigger conditions.</p>

Parameter	Description
Alarm Trigger	The way to trigger alerts for queried results. 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"> • If Suppression is enabled, the query stops after an alert is generated. • If Suppression is disabled, 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

9.4.3 Viewing Available Models

Scenario


This topic describes how to view available models.

Prerequisites

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

Table 9-26 Viewing available models

Parameter	Description
Model Statistics	This area displays how many Available Models and how many Active models you have.
Severity	This bar displays the number of available models by severity levels, including Critical, High, Medium, Low, and Informative.
Model list	The model list displays the severity, name/ID, pipeline name, model type of each model as well as when the model is created and upgraded.

----End

9.4.4 Managing Models

Scenario

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Intelligent Modeling**.
- Step 5** On the **Available Models** tab, manage models.

Table 9-27 Managing models

Operation	Description
Enable	<p>In the model list, click Enable in the Operation column of the target model.</p> <p>NOTE 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>

Operation	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	<ol style="list-style-type: none"> In the model list, locate the row that contains the target model and click Delete in the Operation column. <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> <ol style="list-style-type: none"> In the displayed dialog box, click OK.

----End

9.5 Security Analysis

9.5.1 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.

Cloud services and logs that can be interconnected with SecMaster

SecMaster can integrate logs of multiple cloud products. You can search for and analyze all collected logs in SecMaster.

For details, see [Log Access Supported by SecMaster](#).

9.5.2 How to Use Security Analysis

[Table 9-28](#) shows the process of using the security analysis function.

Table 9-28 Process

Step	Description
Adding a Workspace	Add a workspace for resource isolation and control.

Step	Description
Integrating Data	Configure the source of security data you need to collect. 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.

9.5.3 Log Fields

This section describes the meaning of each field.

- **Common Fields**: describes common fields.
- **sec-waf-attack**: describes the fields in WAF attack logs.
- **sec-waf-access**: describes the fields in WAF access logs.
- **sec-obs-access**: describes the fields in OBS access logs.
- **sec-nip-attack**: describes the fields in IPS attack logs.
- **sec-iam-audit**: describes the fields in IAM audit logs.
- **sec-hss-vul**: describes the fields in the HSS host vulnerability scan result.
- **sec-hss-alarm**: describes the fields in the HSS host security alerts.
- **sec-hss-log**: describes the fields in the HSS host security logs.
- **sec-ddos-attack**: describes the fields in the DDoS attack logs.

- **sec-cts-audit**: describes the fields in the CTS logs.
- **sec-cfw-risk**: describes the fields in the CFW attack incident logs.
- **sec-cfw-flow**: describes the fields in the CFW traffic logs.
- **sec-cfw-block**: describes the fields in the CFW access control logs.
- **sec-apig-access**: describes the fields in the API Gateway access logs.
- **sec-dbss-alarm**: describes the fields in the DBSS alert logs.
- **sec-dsc-alarm**: describes the fields in the DSC alert logs.

Common Fields

Table 9-29 Common fields

Parameter	Field Type	Description
__time	Date	Time when a log is generated
__raw	String	Raw log
ops.source	String	Data source
ops.rgn	String	Site
ops.csvc	String	Data source (cloud service)
ops.ver	String	Data warehouse version
ops.hash	String	Integrity verification of extend hash value of original
[src_/dest_]asset.domain.id	String	Domain ID
[src_/dest_]asset.domain.name	String	Domain name
[src_/dest_]asset.id	String	Asset ID
[src_/dest_]asset.name	String	Asset name
[src_/dest_]asset.type	String	Asset type
[src_/dest_]asset.region	String	Asset site
[src_/dest_]geo.ip	String	IP address
[src_/dest_]geo.country	String	Country name (Chinese)
[src_/dest_]geo.prov	String	Province name (Chinese)
[src_/dest_]geo.city	String	City name (Chinese)
[src_/dest_]geo.org	String	Organization that registers the IP address

Parameter	Field Type	Description
[src_/dest_]geo.isp	String	Carrier
[src_/dest_]geo.loc.lat	Float	Latitude
[src_/dest_]geo.loc.lon	Float	Longitude
[src_/dest_]geo.tz	Integer	Time zone
[src_/dest_]geo.utc_off	Integer	Time zone
[src_/dest_]geo.cac	String	Time zone
[src_/dest_]geo.iddc	String	International call prefix code
[src_/dest_]geo.cc	String	Country code (ISO)
[src_/dest_]geo.contc	String	Continental code (ISO)
[src_/dest_]geo.idc	String	Data center (equipment room)
[src_/dest_]geo.bs	String	Mobile base station
[src_/dest_]geo.cc3	String	Country code (3 digits)
[src_/dest_]geo.euro	String	EU member states

sec-waf-attack

Fields in WAF attack logs

Table 9-30 sec-waf-attack

Field	Type	Description
category	String	Category. The value is attack .
time	Date	Log time.
time_iso8601	Date	ISO 8601 time of the log.
policy_id	String	Protection policy ID.
level	Integer	Protection policy level. The value can be 1 (loose), 2 (medium), or 3 (strict).

Field	Type	Description
attack	String	<p>Attack type The value can be:</p> <ul style="list-style-type: none"> ● default: default attacks ● xss: cross-site scripting (XSS) attacks ● sqli: SQL injections ● cmdi: command injections ● lfi: local file inclusion attacks ● rfi: remote file inclusion attacks ● webshell: web shells ● robot: crawler attacks (blocked based on the user agent blacklist) ● vuln: vulnerability exploits ● cc: attacks that hit the CC rules ● custom_custom: attacks that hit a precise protection rule ● custom_whiteip: attacks that hit a whitelist rule ● custom_geoip: attacks that hit a geolocation rule ● illegal: unauthorized requests ● anticrawler: attacks that hit the anti-crawler rule, such as JS challenges ● antitamper: attacks that hit a web tamper protection rule ● leakage: attacks that hit a sensitive data protection rule ● followed_action: attacks that hit a known attack source rule ● trojan: Website Trojans

Field	Type	Description
action	String	Processing action. The value can be: <ul style="list-style-type: none"> • block: WAF blocks attacks. • log: WAF only logs detected attacks. • captcha: verification code.
rule	String	ID of the triggered rule or the description of the custom policy type.
sub_type	String	When attack is set to robot , this field cannot be left blank. It indicates the subtype of a crawler. <ul style="list-style-type: none"> • script_tool: script tools • search_engine: search engines • scanner: scanning tools • uncategorized: other crawlers
location	String	Location of the triggered payload.
resp_headers	String	Response header.
resp_body	String	Response body.
hit_data	String	Triggered payload string.
status	String	Status code of the response to the request.
reqid	String	Random ID.
id	String	Attack ID.
method	String	Request method.
sip	String	Request IP address of the client.
sport	String	Request port of the client.
host	String	Domain name of the requested server.
http_host	String	Port number of the requested server.
uri	String	Request URL.

Field		Type	Description
header		String	Request header information.
mutipart		String	Request multipart header (file upload).
cookie		String	Request cookie.
params		String	Parameters following the request URI.
body_bytes_sent		String	Total number of bytes of the response body sent to the client.
upstream_response_time		String	Response time of the backend server.
process_time		String	Detection duration of the engine.
engine_id		String	Unique ID of the engine.
group_id		String	Log group ID used for interconnecting with LTS.
attack_stream_id		String	ID of access_stream of the user in the log group identified by the group_id field.
hostid		String	ID of a protected domain name.
tenantid		String	Tenant ID of the protected domain name.
projectid		String	Project ID of the protected domain name.
backend		Object	Address of the backend server to which the request is forwarded.
backend	type	String	Backend host type (IP address or domain name).
	alive	String	Backend host status.
	host	String	Backend host value.
	protocol	String	Backend protocol.
	port	Integer	Backend port.

sec-waf-access

Table 9-31 describes the fields in WAF access logs.

Table 9-31 sec-waf-access

Field	Type	Description
requestid	String	Random ID
time	Date	Log time
eng_ip	String	Engine IP address
hostid	String	ID of a protected domain name
tenantid	String	Tenant ID of the protected domain name
projectid	String	Project ID of the protected domain name
remote_ip	String	IP address of the client that sends the request
scheme	String	Request protocol type
response_code	String	Response code of a request
method	String	Request method
http_host	String	Domain name of the requested server
url	String	Request URL
request_length	String	Request length
bytes_send	String	Total number of bytes sent to the client
body_bytes_sent	String	Total number of bytes of the response body sent to the client
upstream_addr	String	IP address of the selected backend server
request_time	String	Request processing time, which starts from the first byte sent from the client
upstream_response_time	String	Response time of the backend server
upstream_status	String	Response code of the backend server
upstream_connect_time	String	Duration for connecting to the backend server

Field	Type	Description
upstream_header_time	String	Time used by the backend server to receive the first byte of the response header
bind_ip	String	Retrieval IP address of the engine
engine_id	String	Unique ID of the engine
time_iso8601	Date	ISO 8601 time of the log
sni	String	Domain name requested through the SNI
tls_version	String	Version of the protocol used to establish an SSL connection
ssl_curves	String	List of curves supported by the client
ssl_session_reused	String	Whether an SSL session is reused <ul style="list-style-type: none"> • r: It is reused. • .: It is not used.
process_time	String	Detection duration of the engine
x_forwarded_for	String	Content of X-Forwarded-For in the request header
cdn_src_ip	String	Content of Cdn-Src-Ip in the request header
x_real_ip	String	Content of X-Real-Ip in the request header

sec-obs-access

Fields in OBS access logs

Table 9-32 sec-obs-access

Field	Type	Description
srcip	String	Source IP address for accessing OBS.
srcport	String	Source port for accessing OBS.
logtime	Date	Time when the log is generated.
ces_log_version	String	Version number, which is V0 for an internal request. V0 does not record Cloud Eye audit logs, and V1 records Cloud Eye audit logs.
request_start_time	String	Request start time.

Field	Type	Description
ctx_request_id	String	Request ID, which uniquely identifies a request to be traced.
request_method	String	Request method (GET/POST).
remote_ip	String	Remote IP address, in the format of Client IP address:Port number .
operation	String	Operation type, for example, GET.OBJECT .
bucket_name	String	Bucket name.
object_name	String	Object name (file name).
query_string	String	Request query.
http_status	String	HTTP request status code, for example, 200.
content_length	String	Length of the requested content.
user_agent	String	Client agent.
storage_class	String	OBS storage class.
user_name	String	Username of the requester.
user_id	String	User ID of the requester.
domain_name	String	Domain name of the requester.
domain_id	String	Domain ID of the requester.
project_id	String	Project ID of the requester.
owner_domain_name	String	Tenant name of the bucket owner.
owner_domain_id	String	Tenant ID of the bucket owner.
owner_project_id	String	Project ID of the bucket owner.
transmission_type	String	Network type. The value can be: <ul style="list-style-type: none"> • 1: intranet • 2: public network
scheme	String	Network protocol.
http_version	String	HTTP version.
host	String	OBS domain name.
port	String	Port number.
auth_v2_v4	String	Authentication mode.
host_type	String	Access type.

Field	Type	Description
x_forwarded_for	String	IP address of the proxy client.
pub_bkt	String	Whether the bucket is accessed anonymously.
pub_obj	String	Whether an object is accessed anonymously.
website_req	String	Whether the request is a website request.
crr_req	String	Whether the request is a CRR request.
batch_delete_success_count	String	Number of successful batch deletions.
ctc_log_urn	String	Agency.
requester	String	Agency account.
is_over_write	String	Whether to overwrite data.
error_code	String	Cause of an error.
detail_error_code	String	Detailed error cause.
request_content_type	String	Request object type.
request_content_md5	String	MD5 of the request object.
total_bytes_received	String	Total bytes of received content.
response_content_type	String	Response object type.
total_bytes_sent	String	Total bytes of sent content in the response header and response body.
referrer	String	Reference page.
index_read_count	String	Metadata table query latency.
persistence_read_count	String	Number of times that data is read.
vpc_id	String	ID of the VPC to which the request client belongs.
access_with_security_token	String	Access using the STS token.
copy_size	String	Copy size.
vpcep_traffic	String	Transmission through VPCEP.
access_key	String	AK.

sec-nip-attack

Fields in IPS attack logs

Table 9-33 sec-nip-attack

Field	Type	Description
SyslogId	String	Log serial number (SN).
Vsys	String	Virtual system name.
Policy	String	Name of a security policy.
SrcIp	String	Source IP address of a packet.
DstIp	String	Destination IP address of a packet.
SrcPort	String	Source port of a packet. For an ICMP packet, the value of this field is 0 .
DstPort	String	Destination port of a packet. For an ICMP packet, the value of this field is 0 .
SrcZone	String	Source security zone of a packet.
DstZone	String	Destination security zone of a packet.
User	String	Username.
Protocol	String	Protocol of the packet detected by a signature.
Application	String	Application that the packet detected by a signature belongs to.
Profile	String	Name of a configuration file.
SignName	String	Name of a signature.
SignId	String	ID of a signature.
EventNum	String	The field is used for log mergence. Whether logs are merged is determined by the mergence frequency and conditions. The value is 1 if logs are not merged.
Target	String	Object attacked by the packet detected by a signature. The value can be: <ul style="list-style-type: none"> • server: The attack object is the server. • client: The attack object is the client. • both: The attack objects are both the server and client.

Field	Type	Description
Severity	String	Severity of the attack caused by the packet detected by a signature. The value can be: <ul style="list-style-type: none"> • information • low • medium • high
Os	String	OS attacked by the packet detected by a signature. The value can be: <ul style="list-style-type: none"> • all: all OSs • android: Android • ios: iOS • unix-like: Unix • windows: Windows • other: other OSs
Category	String	Threat type of the detected attack packet features.
Action	String	Signature action. <ul style="list-style-type: none"> • Alert • Block
Reference	String	Reference information about the signature.
Extend	String	Evidence collection field in enhanced mode.

sec-iam-audit

Fields in IAM audit logs

Table 9-34 sec-iam-audit

Field	Type	Description
uid	String	User ID
un	String	Username
did	String	Domain ID
dn	String	Domain name
src	String	Request domain name

Field	Type	Description
opl	String	Operation level
op	String	Operation type
res	String	IAM service invoking result
ter	String	Source IP address
dtl	String	IAM authentication details
tn	Date	Occurrence time
ts	Long	Timestamp when the IAM service is invoked
tid	String	Trace ID
evnt	String	Incident
tobj	String	Service

sec-hss-vul

Fields in HSS vulnerability scanning results

Table 9-35 sec-hss-vul

Field	Type	Description
agentUuid	String	Agent UUID.
alarmCsn	String	Alert UUID, which is randomly generated when the master generates an alert.
alarmKey	String	Alert keyword. For an alert, it is the msg_id reported by the transparent transmission agent. For a vulnerability, it is generated by the master.
alarmVersion	String	Agent version.
occurTime	Int64	Vulnerability detection time (ms).
severity	Int32	Vulnerability level defined by HSS.
hostUuid	String	UUID of the affected host.
hostName	String	Name of the affected host.

Field		Type	Description
hostIp		String	Communication IP address of the affected host.
ipList		String	List of IP addresses of affected hosts.
cloudId		String	Cloud agent SN.
region		String	Region where the affected host is located.
projectId		String	ID of the affected tenant.
enterpriseProjectId		String	ID of the affected enterprise tenant.
appendInfo		Object	Vulnerability details.
appendInfo	vulId	String	Official vulnerability ID.
	type	Int32	Vulnerability type. The value can be: <ul style="list-style-type: none"> ● 0: Linux ● 1: Windows ● 2: Web CMS
	repairNecessity	Int32	Necessity level of vulnerability fixing. The value can be: <ul style="list-style-type: none"> ● 1: low-risk ● 2&3: medium-risk ● 4: high risk
	status	Int32	Reserved field.
	cve_ids	String	CVE ID list. Use commas (,) to separate CVE IDs.
	url	String	URL of the official website where the vulnerability details are available.
	vulNameEn	String	Vulnerability name in English.
	vulNameCn	String	Vulnerability name in Chinese.
	severityLevel	String	Vulnerability severity. The options are as follows: <ul style="list-style-type: none"> ● Critical ● High ● Medium ● Low

Field	Type	Description
descriptionEn	String	Vulnerability description in English.
descriptionCn	String	Vulnerability description in Chinese.
solutionEn	String	Solution description in English.
solutionCn	String	Solution description in Chinese.
repairCmd	String	Fix command.
needBoot	Int32	Whether to restart the system. The default value is 1 , which means not to restart the system.
errorInfo	String	Fix failure cause.
appName	String	Name of the software that has the vulnerability (only for Linux vulnerabilities).
version	String	Version of the software that has the vulnerability (only for Linux vulnerabilities).
createTime	Int64	First detection time (ms).
updateTime	Int64	Vulnerability fixing time (ms). The initial value is the same as that of createTime .
agentId	String	UUID of the associated host agent.
projectId	String	ID of the affected tenant.

sec-hss-alarm

Fields in HSS alert logs

Table 9-36 sec-hss-alarm

Field	Type	Description
agentUuid	String	Agent UUID.
alarmCsn	String	Alert UUID.

Field	Type	Description	
alarmKey	String	Alert keyword. For an alert, it is the msg_id reported by the transparent transmission agent. For a vulnerability, it is generated by the master.	
alarmVersion	String	Agent version.	
occurTime	Long	Incident occurrence time (accurate to millisecond).	
severity	Long	Severity.	
hostUuid	String	UUID of the affected host.	
hostName	String	Name of the affected host.	
hostIp	String	Communication IP address of the affected host.	
ipList	String	List of IP addresses of affected hosts.	
cloudId	String	Cloud agent SN.	
region	String	Region where the affected host is located.	
projectId	String	ID of the affected tenant.	
enterpriseProjectId	String	ID of the affected enterprise tenant.	
appendInfo	Object	Alert details.	
appendInfo	agent_id	String	Agent ID.
	version	String	Incident version.
	container_name	String	Container ID (in container security scenarios).
	image_name	String	Image name (in container security scenarios).
	event_id	String	Incident ID (GUID).
	event_name	String	Incident name.
	event_classid	String	Unique incident ID.
	occur_time	Long	Occurrence time (accurate to second).
recent_time	Long	Last occurrence time (accurate to second).	

Field		Type	Description
	event_category	Integer	Incident category.
	event_type	Integer	Incident type.
	event_count	Integer	Number of incidents.
	severity	Integer	Severity.
	attack_phase	Integer	Attack phase.
	attack_tag	Integer	Attack tag.
	confidence	Integer	Confidence.
	action	Integer	Action.
	detect_module	String	Detection module.
	report_source	String	Report source.
	related_events	String	Related incident ID.
	resource_info	Object	Resource information.
	network_info	Object	Network information.
	app_info	Object	Application information.
	system_info	Object	System information.
	process_info	list	Process information.
	user_info	list	User information.
	file_info	list	File information.
	geo_info	Object	Geographic information.
	malware_info	Object	Malware information.
	forensic_info	String	Evidence collection field.
	recommendation	String	Handling suggestions.
	extend_info	String	Extended incident information.
resource_info	project_id	String	Project ID.
	region_name	String	Region name.
	vpc_id	String	VPC ID.
	host_name	String	Host name.
	host_ip	String	Host IP address.
	host_id	String	Host ID (ECS ID).

Field		Type	Description	
		cloud_id	String	Cloud agent SN.
		vm_name	String	VM name.
		vm_uuid	String	VM UUID.
		container_id	String	Container ID.
		image_id	String	Image ID.
		sys_arch	String	System CPU architecture.
		os_bit	String	OS bit version.
		os_type	String	OS type.
		os_name	String	OS name.
		os_version	String	OS version.
	network_info	local_address	String	Local address.
		local_port	Integer	Local port.
		remote_address	String	Remote address.
		remote_port	Integer	Remote port.
		src_ip	String	Source IP address.
		src_port	Integer	Source port.
		src_domain	String	Source domain.
		dest_ip	String	Destination IP address.
		dest_port	Integer	Destination port.
		dest_domain	String	Destination domain.
	app_info	sql	String	Executed SQL statement.

Field		Type	Description	
		domain_name	String	DNS domain name.
		url_path	String	URL.
		url_method	String	URL method.
		req_refer	String	URL request referrer.
		email_subject	String	Email subject.
		email_sender	String	Email sender.
		email_recipient	String	Email recipient.
		email_keyword	String	Email keyword.
	process_info	process_name	String	Process name.
		process_path	String	Process file path.
		process_pid	Integer	Process ID.
		process_uid	Integer	Process user ID.
		process_username	String	Process username.
		process_commandline	String	Process file command line.
		process_filename	String	Process file name.
		process_start_time	Long	Process start time.
		process_gid	Integer	Process group ID.
		process_egid	Integer	Effective process group ID.
process_euid	Integer	Effective process user ID.		

Field		Type	Description
	parent_process_name	String	Parent process name.
	parent_process_path	String	Parent process file path.
	parent_process_pid	Integer	Parent process ID.
	parent_process_uid	Integer	Parent process user ID.
	parent_process_cmdline	String	Parent process file command line.
	parent_process_filename	String	Parent process file name.
	parent_process_start_time	Long	Parent process start time.
	parent_process_gid	Integer	Parent process group ID.
	parent_process_egid	Integer	Effective parent process group ID.
	parent_process_euid	Integer	Effective parent process user ID.
	child_process_name	String	Subprocess name.
	child_process_path	String	Subprocess file path.
	child_process_pid	Integer	Subprocess ID.
	child_process_uid	Integer	Subprocess user ID.
	child_process_cmdline	String	Subprocess file command line.

Field		Type	Description	
		child_process_filename	String	Subprocess file name.
		child_process_start_time	Long	Subprocess start time.
		child_process_gid	Integer	Subprocess group ID.
		child_process_egid	Integer	Effective subprocess group ID.
		child_process_euid	Integer	Effective subprocess user ID.
		virt_cmd	String	Virtualization command.
		virt_process_name	String	Virtualization process name.
		escape_mode	String	Escape mode.
		escape_cmd	String	Command executed after the escape.
	user_info	user_id	Integer	User ID.
		user_gid	Integer	User GID.
		user_name	String	Username.
		user_group_name	String	User group name.
		user_home_dir	String	User home directory.
		login_ip	String	User login IP address.
		service_type	String	Login service type.
		service_port	Integer	Login service port.
		login_mode	String	Login mode.
		login_last_time	Long	Last login time of a user.

Field		Type	Description	
		login_fail_count	Integer	Failed login attempts.
		pwd_hash	String	Password hash.
		pwd_with_fuzzing	String	Anonymized password.
		pwd_used_days	Integer	Password age (days).
		pwd_min_days	Integer	Minimum password validity period.
		pwd_max_days	Integer	Maximum password validity period.
		pwd_warn_left_days	Integer	Advance warning of password expiration (days).
	file_info	file_path	String	File path/name.
		file_alias	String	File alias.
		file_size	Integer	File size.
		file_mtime	Long	Time when the file is last modified.
		file_atime	Long	Time when the file is last accessed.
		file_ctime	Long	Time when the file status last changes.
		file_hash	String	File hash value.
		file_md5	String	File MD5 value.
		file_sha256	String	File SHA256 value.
		file_type	String	File type.
		file_content	String	File content.
		file_attr	String	File attribute.
file_operation	String	File operation type.		
file_change_attr	String	Old/New attribute.		

Field		Type	Description	
		file_new_path	String	New file path.
		file_desc	String	File description.
		file_key_word	String	File keyword.
		is_dir	Boolean	Whether the file is a directory.
		fd_info	String	File handle information.
		fd_count	Integer	Number of file handles.
	forensic_info	monitor_process	String	Monitoring process.
		escape_mode	String	Escape mode.
		abnormal_port	String	Abnormal port.
	geo_info	src_country	String	Source country/region.
		src_city	String	Source city.
		src_latitude	Long	Source latitude.
		src_longitude	Long	Source longitude.
		dest_country	String	Destination country/region.
		dest_city	String	Destination city.
		dest_latitude	Long	Destination latitude.
		dest_longitude	Long	Destination longitude.
	malware_info	malware_family	String	Malware family.
		malware_class	String	Malware classification.
	system_info	pwd_valid	Boolean	Whether the password is valid.
		pwd_min_len	Integer	Password length.

Field		Type	Description	
		pwd_digit_credit	Integer	Digits contained in the password.
		pwd_uppercase_letter	Integer	Uppercase letters contained in the password.
		pwd_lowercase_letter	Integer	Lowercase letters contained in the password.
		pwd_special_characters	Integer	Special characters contained in the password.
	extend_info	hit_rule	String	Hit rule.
		rule_name	String	Rule name.
		rulesetname	String	Rule set name.
		report_type	String	Reported data type.
	ti_info	ti_source	String	Intelligence source.
		ti_class	String	Intelligence classification.
		ti_threat_type	String	Intelligence threat type.
		ti_first_time	Long	First detection time.
		ti_last_time	Long	Last detection time.

sec-hss-log

Fields in HSS security logs

Table 9-37 sec-hss-log

Field	Type	Description
agentUuid	String	Agent UUID.
alarmCsn	String	Alert UUID.

Field	Type	Description	
alarmKey	String	Alert keyword. For an alert, it is the msg_id reported by the transparent transmission agent. For a vulnerability, it is generated by the master.	
alarmVersion	String	Agent version.	
occurTime	Long	Incident occurrence time (accurate to millisecond).	
severity	Long	Severity.	
hostUuid	String	UUID of the affected host.	
hostName	String	Name of the affected host.	
hostIp	String	Communication IP address of the affected host.	
ipList	String	List of IP addresses of affected hosts.	
cloudId	String	Cloud agent SN.	
region	String	Region where the affected host is located.	
projectId	String	ID of the affected tenant.	
enterpriseProjectId	String	ID of the affected enterprise tenant.	
appendInfo	Object	Alert details.	
appendInfo	agent_id	String	Agent ID.
	version	String	Incident version.
	container_name	String	Container ID (in container security scenarios).
	image_name	String	Image name (in container security scenarios).
	event_id	String	Incident ID (GUID).
	event_name	String	Incident name.
	event_classid	String	Unique incident ID.
	occur_time	Long	Occurrence time (accurate to second).
recent_time	Long	Last occurrence time (accurate to second).	

Field		Type	Description
	event_category	Integer	Incident category.
	event_type	Integer	Incident type.
	event_count	Integer	Number of incidents.
	severity	Integer	Severity.
	attack_phase	Integer	Attack phase.
	attack_tag	Integer	Attack tag.
	confidence	Integer	Confidence.
	action	Integer	Action.
	detect_module	String	Detection module.
	report_source	String	Report source.
	related_events	String	Related incident ID.
	resource_info	Object	Resource information.
	network_info	Object	Network information.
	app_info	Object	Application information.
	system_info	Object	System information.
	process_info	list	Process information.
	user_info	list	User information.
	file_info	list	File information.
	geo_info	Object	Geographic information.
	malware_info	Object	Malware information.
	forensic_info	String	Evidence collection field.
	recommendation	String	Handling suggestions.
	extend_info	String	Extended incident information.
resource_info	project_id	String	Project ID.
	region_name	String	Region name.
	vpc_id	String	VPC ID.
	host_name	String	Host name.
	host_ip	String	Host IP address.
	host_id	String	Host ID (ECS ID).

Field		Type	Description	
		cloud_id	String	Cloud agent SN.
		vm_name	String	VM name.
		vm_uuid	String	VM UUID.
		container_id	String	Container ID.
		image_id	String	Image ID.
		sys_arch	String	System CPU architecture.
		os_bit	String	OS bit version.
		os_type	String	OS type.
		os_name	String	OS name.
		os_version	String	OS version.
	network_info	local_address	String	Local address.
		local_port	Integer	Local port.
		remote_address	String	Remote address.
		remote_port	Integer	Remote port.
		src_ip	String	Source IP address.
		src_port	Integer	Source port.
		src_domain	String	Source domain.
		dest_ip	String	Destination IP address.
		dest_port	Integer	Destination port.
		dest_domain	String	Destination domain.
app_info	protocol	String	Protocol.	
	app_protocol	String	Application layer protocol.	
	flow_direction	String	Flow direction.	
	sql	String	Executed SQL statement.	

Field		Type	Description	
		domain_name	String	DNS domain name.
		url_path	String	URL.
		url_method	String	URL method.
		req_refer	String	URL request referrer.
		email_subject	String	Email subject.
		email_sender	String	Email sender.
		email_recipient	String	Email recipient.
		email_keyword	String	Email keyword.
	process_info	process_name	String	Process name.
		process_path	String	Process file path.
		process_pid	Integer	Process ID.
		process_uid	Integer	Process user ID.
		process_username	String	Process username.
		process_commandline	String	Process file command line.
		process_filename	String	Process file name.
process_start_time	Long	Process start time.		
process_gid	Integer	Process group ID.		
process_egid	Integer	Effective process group ID.		
process_euid	Integer	Effective process user ID.		

Field		Type	Description
	parent_process_name	String	Parent process name.
	parent_process_path	String	Parent process file path.
	parent_process_pid	Integer	Parent process ID.
	parent_process_uid	Integer	Parent process user ID.
	parent_process_cmdline	String	Parent process file command line.
	parent_process_filename	String	Parent process file name.
	parent_process_start_time	Long	Parent process start time.
	parent_process_gid	Integer	Parent process group ID.
	parent_process_egid	Integer	Effective parent process group ID.
	parent_process_euid	Integer	Effective parent process user ID.
	child_process_name	String	Subprocess name.
	child_process_path	String	Subprocess file path.
	child_process_pid	Integer	Subprocess ID.
	child_process_uid	Integer	Subprocess user ID.
	child_process_cmdline	String	Subprocess file command line.

Field		Type	Description
		child_process_filename	String Subprocess file name.
		child_process_start_time	Long Subprocess start time.
		child_process_gid	Integer Subprocess group ID.
		child_process_egid	Integer Effective subprocess group ID.
		child_process_euid	Integer Effective subprocess user ID.
		virt_cmd	String Virtualization command.
		virt_process_name	String Virtualization process name.
		escape_mode	String Escape mode.
		escape_cmd	String Command executed after the escape.
	user_info	user_id	Integer User ID.
		user_gid	Integer User GID.
		user_name	String Username.
		user_group_name	String User group name.
		user_home_dir	String User home directory.
		login_ip	String User login IP address.
		service_type	String Login service type.
		service_port	Integer Login service port.
		login_mode	String Login mode.
		login_last_time	Long Last login time of a user.

Field		Type	Description	
		login_fail_count	Integer	Failed login attempts.
		pwd_hash	String	Password hash.
		pwd_with_fuzzing	String	Anonymized password.
		pwd_used_days	Integer	Password age (days).
		pwd_min_days	Integer	Minimum password validity period.
		pwd_max_days	Integer	Maximum password validity period.
		pwd_warn_left_days	Integer	Advance warning of password expiration (days).
	file_info	file_path	String	File path/name.
		file_alias	String	File alias.
		file_size	Integer	File size.
		file_mtime	Long	Time when the file is last modified.
		file_atime	Long	Time when the file is last accessed.
		file_ctime	Long	Time when the file status last changes.
		file_hash	String	File hash value.
		file_md5	String	File MD5 value.
		file_sha256	String	File SHA256 value.
		file_type	String	File type.
		file_content	String	File content.
		file_attr	String	File attribute.
file_operation	String	File operation type.		
file_change_attr	String	Old/New attribute.		

Field		Type	Description	
		file_new_path	String	New file path.
		file_desc	String	File description.
		file_key_word	String	File keyword.
		is_dir	Boolean	Whether the file is a directory.
		fd_info	String	File handle information.
		fd_count	Integer	Number of file handles.
	forensic_info	monitor_process	String	Monitoring process.
		escape_mode	String	Escape mode.
		abnormal_port	String	Abnormal port.
	geo_info	src_country	String	Source country/region.
		src_city	String	Source city.
		src_latitude	Long	Source latitude.
		src_longitude	Long	Source longitude.
		dest_country	String	Destination country/region.
		dest_city	String	Destination city.
		dest_latitude	Long	Destination latitude.
		dest_longitude	Long	Destination longitude.
	malware_info	malware_family	String	Malware family.
		malware_class	String	Malware classification.
	system_info	pwd_valid	Boolean	Whether the password is valid.
		pwd_min_len	Integer	Password length.

Field		Type	Description	
		pwd_digit_credit	Integer	Digits contained in the password.
		pwd_uppercase_letter	Integer	Uppercase letters contained in the password.
		pwd_lowercase_letter	Integer	Lowercase letters contained in the password.
		pwd_special_characters	Integer	Special characters contained in the password.
	extend_info	hit_rule	String	Hit rule.
		rule_name	String	Rule name.
		rulesetname	String	Rule set name.
		report_type	String	Reported data type.
	ti_info	ti_source	String	Intelligence source.
		ti_class	String	Intelligence classification.
		ti_threat_type	String	Intelligence threat type.
		ti_first_time	Long	First detection time.
		ti_last_time	Long	Last detection time.

sec-ddos-attack

Fields in Anti-DDoS attack logs

Table 9-38 sec-ddos-attack

Field	Type	Description
log_type	String	Log type
time	Date	local time
device_ip	String	Device IP address

Field	Type	Description
device_type	String	Device type (CLEAN : cleaning device; DETECT : detecting device)
direction	String	Log direction (inbound , outbound)
zone_id	String	Protected object ID
zone_name	String	Protected object name
zone_ip	String	IP address
biz_id	String	Business ID
is_deszone	String	Whether the traffic is network segment traffic (true , false)
is_ipLocation	String	Whether the traffic is geographical location traffic (true , false)
ipLocation_id	String	Geographical location ID
total_pps	String	Total pps
total_kbps	String	Total rate in kbps
tcp_pps	String	Rate of TCP packets to the target (in pps)
tcp_kbps	String	Rate of TCP traffic to the target (in kbps)
tcpfrag_pps	String	Rate of TCP fragments to the target (in pps)
tcpfrag_kbps	String	Rate of TCP fragment traffic to the target (in kbps)
udp_pps	String	Rate of UDP packets to the target (in pps)
udp_kbps	String	Rate of UDP traffic to the target (in kbps)
udpfrag_pps	String	Rate of UDP fragments to the target (in pps)
udpfrag_kbps	String	Rate of UDP fragment traffic to the target (in kbps)
icmp_pps	String	Rate of ICMP packets to the target (in pps)
icmp_kbps	String	Total ICMP traffic to the target (in kbps)
other_pps	String	Rate of OTHER packets to the target (in pps)

Field	Type	Description
other_kbps	String	Total OTHER traffic to the target (in kbps)
syn_pps	String	Number of SYN packets to the target (in pps)
synack_pps	String	Number of SYN/ACK packets to the target (in pps)
ack_pps	String	Rate of ACK packets to the target (in pps)
finrst_pps	String	Rate of FIN/Rst packets to the target (in pps)
http_pps	String	Rate of HTTP packets to the target (in pps)
http_kbps	String	Rate of HTTP traffic to the target (in kbps)
http_get_pps	String	Total packet rate of HTTP requests to the target (in pps)
https_pps	String	Rate of HTTPS packets to the target (in pps)
https_kbps	String	Rate of HTTPS traffic to the target (in kbps)
dns_request_pps	String	Rate of DNS Query packets to the target (in pps)
dns_request_kbps	String	Rate of DNS Query traffic to the target (in kbps)
dns_reply_pps	String	Rate of DNS Reply packets to the target (in pps)
dns_reply_kbps	String	Rate of DNS Reply traffic to the target (in kbps)
sip_invite_pps	String	Rate of SIP packets to the target (in PPS).
sip_invite_kbps	String	Rate of SIP traffic to the target (in kbps)
tcp_increase_con	String	Number of new TCP connections to the target per second
udp_increase_con	String	Number of new UDP connections to the target per second
icmp_increase_con	String	Number of new ICMP connections to the target per second

Field	Type	Description
other_increase_con	String	Number of OTHER connections to the target per second
tcp_concur_con	String	Number of concurrent TCP connections to the target
udp_concur_con	String	Number of concurrent UDP connections to the target
icmp_concur_con	String	Number of concurrent ICMP connections to the target
other_concur_con	String	Number of concurrent OTHER connections to the target
total_average_pps	String	Average pps of all traffic to the target
total_average_kbps	String	Average Kbps of all traffic to the target

sec-cts-audit

Fields in CTS logs

Table 9-39 sec-cts-audit

Field	Type	Description
time	Date	Time when an incident occurs. The value is the local standard time (GMT +local time zone), for example, 2022/11/08 11:24:04 GMT+08:00.
user	Object	Cloud account used to perform the recorded operation.
request	Object	Requested operation.
response	Object	Response to the request.
service_type	String	Operation source.
resource_type	String	Resource type.
resource_name	String	Resource name.
resource_id	String	Unique resource ID.
source_ip	String	IP address of the user who performs an operation. The value of this parameter is empty if the operation is triggered by the system.

Field	Type	Description
trace_name	String	Operation name.
trace_rating	String	Level of an operation incident. The options are as follows: <ul style="list-style-type: none"> • normal: The operation succeeded. • warning: The operation failed. • incident: The operation caused a serious consequence, for example, a node failure or service interruption.
trace_type	String	Operation type. The options are as follows: <ul style="list-style-type: none"> • ConsoleAction: operations performed on the management console • SystemAction: operations triggered by system • ApiCall: operations triggered by invoking API Gateway • ObsSDK: operations on OBS buckets, which were triggered by calling OBS SDKs • Others: operations on OBS buckets except those triggered by calling OBS SDKs
api_version	String	API version of the cloud service on which an operation was performed.
message	Object	Supplementary information.
record_time	Long	Time when the operation was recorded, in the form of a timestamp.
trace_id	String	Unique operation ID.
code	Integer	HTTP return code, for example, 200 or 400.
request_id	String	Request ID.
location_info	String	Additional information required for fault locating after a request error.
endpoint	String	Endpoint of the page that displays details of cloud resources involved in this operation.
resource_url	String	Access link (excluding the endpoint) of the page that displays details of cloud resources involved in this operation.

Field	Type	Description
user_agent	String	Type of OBS bucket-related operations that are not invoked using OBS SDKs.
content_length	Long	Length of the request body for performing operations on OBS buckets.
total_time	Long	Response time of the request in OBS bucket-related operations.

sec-cfw-risk

Fields in CFW attack event logs

Table 9-40 sec-cfw-risk

Field	Type	Description
event_time	Date	Attack time
action	String	Response action of CFW <ul style="list-style-type: none"> • permit • deny
app	String	Application type
attack_rule	String	Defense rule that works for the detected attack
attack_rule_id	String	ID of the defense rule that works for the detected attack

Field	Type	Description
attack_type	String	Type of the attack <ul style="list-style-type: none"> • Vulnerability exploit • Vulnerability scan • Trojan • Worms • Phishing • Web attacks • Application DDoS • Buffer overflow • Password attacks • Mail • Access control • Hacking tools • Hijacking • Protocol exception • Spam • Spyware • DDoS flood • Suspicious DNS activities • Other suspicious behaviors
dst_ip	String	Destination IP address
dst_port	String	Destination port number
packet	String	Original data packet of the attack log
protocol	String	Protocol type
level	String	Level of detected threats <ul style="list-style-type: none"> • CRITICAL • HIGH • MIDDLE • LOW
source	String	Defense for the detected attack <ul style="list-style-type: none"> • 0: basic defense • 1: virtual patch
src_ip	String	Source IP address
src_port	String	Source port number

Field	Type	Description
direction	String	Flow direction <ul style="list-style-type: none"> • out2in: inbound • in2out: outbound

sec-cfw-flow

Fields in CFW traffic logs

Table 9-41 sec-cfw-flow

Field	Type	Description
app	String	Application type
dst_ip	String	Destination IP address
dst_port	String	Destination port number
end_time	Date	Flow end time
protocol	String	Protocol type
to_c_bytes	String	Number of bytes sent from the server to the client
to_c_pkts	String	Number of packets sent from the server to the client
to_s_bytes	String	Number of bytes sent from the client to the server
to_s_pkts	String	Number of packets sent from the server to the client
src_ip	String	Source IP address
src_port	String	Source port number
start_time	Date	Flow start time

sec-cfw-block

Fields in CFW access control logs

Table 9-42 sec-cfw-block

Field	Type	Description
hit_time	Date	Time of access

Field	Type	Description
action	String	Response action of CFW <ul style="list-style-type: none"> • permit • deny
app	String	Application type
dst_ip	String	Destination IP address
dst_port	String	Destination port number
protocol	String	Protocol type
rule_id	String	ID of the triggering rule
src_ip	String	Source IP address
src_port	String	Source port number

sec-apig-access

Fields in API Gateway access logs

Table 9-43 sec-apig-access

Field	Type	Description
region_id	String	Site.
api_id	String	API ID.
body_bytes_sent	String	Response body size.
bytes_sent	String	Size of the entire response.
domain	String	Public network domain name.
errorType	String	Status of request throttling. Value 1 indicates that request throttling is enabled.
http_user_agent	String	User agent ID.
http_x_forwarded_for	String	X-Forwarded-For header.
opsuba_api_url	String	Request URI.
out_times	String	Time required for interaction between the gateway and peripheral components.
remote_addr	String	Remote IP address.
request_id	String	Request ID.

Field	Type	Description
request_length	String	Size of the entire request.
request_method	String	HTTP request method.
request_time	String	Time required for access.
scheme	String	Protocol.
server_protocol	String	Request protocol.
status	String	Status.
time_local	Date	Time.
upstream_addr	String	Remote IP address.
upstream_connect_time	String	Time required for a remote connection.
upstream_header_time	String	Time required for receiving the header at the remote end.
upstream_response_time	String	Time required for returning a response from the remote end.
upstream_status	String	Remote status.
upstream_uri	String	Request backend URI.
user_name	String	Project ID or app ID of the user.

sec-dbss-alarm

Fields in DBSS alert logs

Table 9-44 dbss-alarm

Field	Type	Description
domain_id	String	Account ID.
project_id	String	Project ID
region	String	Region
tenant_vpc_id	String	VPC ID of the tenant
tenant_subnet_id	String	Subnet ID of the tenant
instance_id	String	Instance ID
instance_name	String	Instance name
alarm	Object	Alert object

Field		Type	Description
source_type		String	DBSS
alarm	alarm_risk	String	Severity
	client_ip	String	Connection IP address
	database_ip	String	IP address for accessing the database
	count	Long	Number of alerts
	user_name	String	Database username
	schema	String	Oracle schema
	rule_name	String	Rule name
	rule_id	String	Rule ID
	sql_type	String	SQL execution type
	sql_result	String	SQL execution result
db_type	String	Database type	

sec-dsc-alarm

The reserved fields in DSC alert logs vary depending on the log types.

Table 9-45 AK SK leakage (aksk_leakage)

Field	Type	Description
log_type	String	Alert type
region_id	String	Region
domain_id	String	Account ID.
project_id	String	Project ID
leakage_ak	String	AK
source	String	Leakage source
find_time	String	Discovery time
account	String	Account name.
file_name	String	File name
file_suffix	String	File name extension
leakage_user_id	String	Sub-user ID of the leakage

Field	Type	Description
leakage_user_name	String	Sub-username of the leakage
leakage_domain_id	String	Leaked account ID.
leakage_domain_name	String	Leaked account name.
url	String	Website URL of the leakage

Table 9-46 Risky OBS bucket files (obs_risk)

Field	Type	Description
log_type	String	Alert type
region_id	String	Region
domain_id	String	Account ID.
project_id	String	Project ID
bucket_policy	String	Public bucket/Private bucket
bucket_domain_id	String	ID of the account that the bucket belongs to.
bucket_project_id	String	ID of the project to which the bucket belongs
bucket_name	String	Bucket name
file_name	String	File name
file_path	String	File path
risk_level	Integer	Sensitive risk level
sensitive_data_type	String[]	Sensitive data type
privacy_detail	String	Personal privacy data details
file_type	String	File type
mimetypes	String	File type
rule_list	List<Map<String,String>>	List of matched rules
keyword	String	Keyword for matching sensitive data rules
available_zone	String	AZ
encrypted	String	Whether to encrypt data

Table 9-47 Sensitive data fields (db_risk)

Field	Type	Description
log_type	String	Alert type
region_id	String	Region
domain_id	String	Account ID.
project_id	String	Project ID
vpc_id	String	VPC ID
db_instance_type	String	RDS PUB
db_instance_id	String	Database instance ID
db_instance_type	String	Database instance type
db_instance_ip	String	IP address of the database instance
db_instance_domain_id	String	ID of the account that the database instance belongs to.
db_instance_project_id	String	ID of the project to which the database instance belongs
db_instance_name	String	Database instance name
db_name	String	Database name
table_name	String	Table name
field_name	String	Field name
data_type	String	Field data type
risk_level	Integer	Sensitive risk level
sensitive_data_type	String[]	Sensitive data type
privacy_detail	String	Personal privacy data details
rule_list	List<Map<String,String>>	List of matched rules
keyword	String	Keyword for matching sensitive data rules

9.5.4 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**.

Limitations and Constraints

Custom index can be configured only for new custom pipelines. For details, see [Creating a Pipeline](#).

Configuring Field Indexes


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- 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.
- 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 9-48](#).

Table 9-48 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.

Parameter	Description
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

9.5.5 Querying and Analyzing Data

Scenario

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.


- [Executing a Query and Analysis Based on Query Criteria](#)
- [Using Existing Fields for Query and Analysis](#)
- [Managing Query Analysis Results](#)

Prerequisites

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

Executing a Query and Analysis Based on Query Criteria

Step 1 Log in to the management console.

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

- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- 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.
- 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 Statements - SQL Syntax](#).

 **NOTE**

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

- 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 part of the page and choose **Security > SecMaster**.

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




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

- 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.

- 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.

- In raw logs, click  before an optional field on the left and click  (adding a field value) next to the field to search for specific logs that contain the selected field value. To exclude a field value, click  before the field name.

- If you have expanded the log data at a specific time point and need to filter some fields, click ⊕ (adding a field value) in front of the field name. The query box displays the matched fields. To exclude a field value, click ⊖ before the field name.

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](#).

9.5.6 Downloading Logs



Scenario

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- 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.
- 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

9.5.7 Query and Analysis Statements - SQL Syntax

9.5.7.1 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 9-49 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 statements	An analysis statement is used to calculate and collect statistics on query results.

9.5.7.2 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.

9.5.7.3 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 9-50 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 9-51 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'

Query Requirement	Query Statement
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

9.5.7.4 Analysis Statements - SELECT

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 indicates the field to be queried. The following part describes parameters and examples for the **SELECT** syntax.

Using * to query all fields.

```
SELECT *
```

Table 9-52 Using * to query all fields

account_number	firstname	gender	city	balance	employer	state	lastname	age
1	Ambler	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 9-53 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 9-54 Using AS to define field aliases

num
1
16
13
18

Using the DISTINCT Statement

```
SELECT DISTINCT age
```

Table 9-55 Using the DISTINCT statement

age
32
36
28

Using SQL Functions

For details about functions, see [Functions](#).

```
SELECT LENGTH(firstname) as len, firstname
```

Table 9-56 Using SQL functions

len	firstname
4	Amber
6	Hattie
7	Nanette
4	Dale

9.5.7.5 Analysis Statements - GROUP BY

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]
```

Where, **GROUP BY** indicates grouping by value. The following part describes parameters and examples for the **GROUP BY** syntax.

Grouping by Field Value

```
SELECT age GROUP BY age
```

Table 9-57 Grouping by field value

age
28
32
36

Grouping by Field Alias

```
SELECT account_number AS num GROUP BY num
```

Table 9-58 Grouping by field alias

num
1
16
13
18

Grouping by Multiple Fields

```
SELECT account_number AS num, age GROUP BY num, age
```

Table 9-59 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 9-60 Using SQL functions

len	count
4	2
5	2

9.5.7.6 Analysis Statements - HAVING

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]
```

The **HAVING** syntax specifies the conditions for filtering group results (**GROUP BY**) or aggregation calculation results. The following part describes parameters and examples for the **HAVING** syntax.

Filters data based on grouping and [Aggregate Functions](#).

```
SELECT age, MAX(balance) GROUP BY age HAVING MIN(balance) > 10000
```

Table 9-61 The HAVING function

age	MAX(balance)
28	32838
32	39225

9.5.7.7 Analysis Statements - ORDER BY

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]
```

Where, **ORDER BY** indicates sorting by field value. The following part describes parameters and examples for the **ORDER BY** syntax.

Sorting Data by Field Value

```
SELECT age ORDER BY age DESC
```

Table 9-62 Sorting by field value

age
28
32
32
36

9.5.7.8 Analysis Statements - LIMIT

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]
```

Where, **LIMIT** indicates the number of returned data records. The following part describes parameters and examples for the **LIMIT** syntax.

Specifying the Number of Returned Records

```
SELECT * LIMIT 1
```

Table 9-63 Specifying the number of returned records

account_number	first_name	gender	city	balance	employer	state	last_name	age
1	Ambler	M	Brogan	39225	Pyrami	IL	Duke	32

Specifying the Number of Returned Records and Offsets

```
SELECT * LIMIT 1 OFFSET 1
```

Table 9-64 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	Netagy	TN	Bond	36

9.5.7.9 Analysis Statements - Functions

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]
```

This section describes functions.

Mathematics Functions

Table 9-65 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

Function	Purpose	Description	Example Value
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
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 9-66 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 9-67 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 9-68 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 9-69 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

9.5.7.10 Analysis Statements - Aggregate Functions

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]
```

This section describes some aggregate functions.

Table 9-70 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

Function	Purpose	Description	Example Value
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
count	Occurrences	count(field) -> integer , count(*) -> integer , count(1) -> integer	SELECT count(age) LIMIT 1 , SELECT count(*) LIMIT 1 , SELECT count(1) LIMIT 1

9.5.8 Quick Query

Scenario

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- 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.
- 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**.

Table 9-71 Parameters for a quick query

Parameter	Description
Query Name	Set the name of the quick query.
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

9.5.9 Quickly Adding a Log Alarm Model

Scenario

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- 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.
- 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.
- Step 8** Configure basic alarm information by referring to [Table 9-72](#).

Table 9-72 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	The alarm model status. 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 9-73](#).

Table 9-73 Configure Model Logic

Parameter	Description
Query Rule	<p>Set alert query rules. After the setting is complete, click Run and view the running result.</p> <p>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 Statements - SQL Syntax.</p> <p>NOTE If the reserved field is of the text type, MATCH_QUERY is used for word segmentation queries by default.</p>

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 trigger conditions, click Add and add them. A maximum of five trigger conditions can be added.</p> <p>If there are multiple trigger conditions, SecMaster scans log data to hit each trigger condition from top to bottom and generates all types of alerts for hit trigger conditions.</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"> If Suppression is enabled, the query stops after an alert is generated. If Suppression is disabled, 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

9.5.10 Charts

9.5.10.1 Overview

SecMaster supports a wide range of chart types to display query and analysis results. You can select the one you like.

SecMaster can display query and analysis results in the following chart types:

- [Table](#)
- [Line Chart](#)
- [Bar Chart](#)
- [Pie Chart](#)


9.5.10.2 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 part of the page and choose **Security > SecMaster**.

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

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

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.

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  .

Step 8 Set parameters in the table.

Table 9-74 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

- 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.

9.5.10.3 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- 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.
- 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 .
- Step 8** Set line chart parameters.

Table 9-75 Line 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

- 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.


9.5.10.4 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 part of the page and choose **Security > SecMaster**.


- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- 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.
- 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 .
- Step 8** Set bar chart parameters.

Table 9-76 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

- 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.

9.5.10.5 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- 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.
- 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 .
- Step 8** Set pie chart parameters.

Table 9-77 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

- **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.

9.5.11 Managing Data Spaces

9.5.11.1 Creating a Data Space

Scenario

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.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- Step 5** In the upper left corner of the data space list, click **Add**. The **Adding Data Spaces** page is displayed on the right.
- Step 6** On the **Adding Data Spaces** page, set the parameters for the new data space. For details about the parameters, see [Table 9-78](#).

Table 9-78 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


9.5.11.2 Viewing Data Space Details

Scenario

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 part of the page and choose **Security > SecMaster**.

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


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

Step 5 On the **Data Spaces** page, view all data space information. [Table 9-79](#) describes related parameters.

Table 9-79 Data space parameters

Parameter	Description
Data Spaces	Data space name

Parameter	Description
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.

Step 7 In the Data **Space Details** area, you can view details about a data space. For details about the parameters, see [Table 9-80](#).

Table 9-80 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


9.5.11.3 Editing a Data Space

Scenario

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 part of the page and choose **Security > SecMaster**.

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

- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- Step 5** Locate the row that contains the data space to be edited, and click **Edit** in the **Operation** column.
- Step 6** In the displayed **Edit Data Space** dialog box, modify the data space information.
- Step 7** Click **OK**.
- End

9.5.11.4 Deleting a Data Space


Scenario

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- Step 5** In the row containing the desired database, click **Delete** in the **Operation** column.
- Step 6** In the dialog box displayed, click **OK**.

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

9.5.12 Managing Pipelines

9.5.12.1 Creating a Pipeline

Scenario

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](#).

Procedure




- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- 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.
- Step 6** On the **Create Pipeline** page, configure pipeline parameters. For details about the parameters, see [Table 9-81](#).

Table 9-81 Creating a pipeline

Parameter	Description
Data Spaces	Data space to which the pipeline belongs, which is generated by the system by default.
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.

Parameter	Description
Shards	The number of shards of the pipeline. The value range is 1 to 64. An index can potentially store a large amount of data that exceeds the hardware limits of a single node. To solve this problem, Elasticsearch subdivides your index into multiple pieces called shards. When creating an index, you can specify the number of shards as required. Each shard is in itself a fully-functional and independent "index" that can be hosted on any node in the cluster.
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

9.5.12.2 Viewing Pipeline Details

Scenario

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- Step 5** In the data space navigation tree on the left, click a data space name to show the pipeline list.
- Step 6** Click  next to a pipeline name you want to view. The pipe details are displayed in the right pane.

Table 9-82 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

9.5.12.3 Editing a Pipeline

Scenario


After a pipeline is created, you can modify the pipeline information, such as the number of shards, description, and lifecycle.

This topic describes how to modify pipeline parameters.

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.

- Step 5** In the data space navigation tree on the left, click a data space name to show the pipeline list.
- Step 6** Click **More > Edit** next to the pipeline name.
- Step 7** On the **Edit Pipeline** page, set pipeline parameters. For details about the parameters, see [Table 9-83](#).

Table 9-83 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

9.5.12.4 Deleting a Pipeline

Scenario


This section describes how to delete 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- Step 5** In the data space navigation tree on the left, click a data space name to show the pipeline list.

Step 6 Click **More > Delete** next to the pipeline name.

Step 7 In the dialog box displayed, click **OK**.

----End


9.5.13 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 part of the page and choose **Security > SecMaster**.

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

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

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**.

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 9-84](#).

Table 9-84 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. This parameter determines how data is transmitted to data 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.

9.5.14 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 part of the page and choose **Security > SecMaster**.

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

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

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**.

Step 6 On the pipeline monitoring page, view monitoring metrics.

- **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 (B), 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

9.6 Data Delivery

9.6.1 Creating a Data Delivery

Scenario

SecMaster can deliver data to other pipelines or other cloud 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).

This section describes how to create a data delivery task.

Prerequisites


- If you want to deliver data to an OBS bucket, the bucket must have private, public read, or public read/write policy enabled. Currently, parallel file buckets are not supported.
- 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 part of the page and choose **Security > SecMaster**.

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

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

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**.

Step 6 (Optional) Confirm the authorization information, select **Agree to authorize** and click **OK**.

Authorization is required for the first delivery to a specific destination type. If the authorization has been performed, skip this step.

Step 7 On the **Create Delivery** page, set data delivery parameters.

1. Configure basic information.

Table 9-85 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 9-86 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 9-87](#).

Table 9-87 Destination parameters - Current account pipeline

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

Parameter	Description
Data Spaces	Data space where the destination PIPE is located
Pipeline	Pipeline where the destination PIPE is located
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 9-88](#).

Table 9-88 Destination parameters - PIPE of Other account

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 pipeline 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 9-89](#).

To deliver data to LTS, ensure there is an available log group and log streams.

Table 9-89 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.

Parameter	Description
Delivery Type	Delivery type. Select LTS .
Log Group	Destination LTS log group
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 9-90](#).

Note that the OBS bucket you use must have private, public read, or public read/write policy enabled. Currently, parallel file buckets are not supported.

Table 9-90 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.

4. Under **Access Authorization**, view the permissions granted in [Step 6](#).

A delivery request requires the read and write permissions to access your cloud resources. After the authorization, the delivery task can access your cloud resources.

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](#).

9.6.2 Data Delivery Authorization

Scenario

After a data delivery task is added, you need to grant the delivery permission. The delivery takes effect only after you accept the authorization.

This topic describes how to authorize a data delivery.


Prerequisites

Data delivery has been added.

Limitations and Constraints

If the new data delivery is cross-account, you need to log in to SecMaster using the destination account and perform authorization.

Procedure

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

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 9-91 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.

Operation	Description
Cancel	<ol style="list-style-type: none"> 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. In the displayed dialog box, click OK.

9.6.3 Checking the Data Delivery Status

Scenario


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 part of the page and choose **Security > SecMaster**.
 - Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
 - Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
 - 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.
 - 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 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

9.6.4 Managing Data Delivery

Scenario

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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Threat Operations > Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.

Step 5 On the delivery task list page, view existing delivery tasks.


Table 9-92 Delivery task parameters

Operation	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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.
- 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.
- 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. On the page displayed, click the **Data Delivery Management** tab.
- 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

9.6.5 Delivering Logs to LTS

Scenario

SecMaster can integrate logs of other cloud products, such as WAF, HSS, and CFW. For details about how to integrate, see [Data Integration](#).

You can deliver integrated logs to Log Tank Service (LTS) for real-time decision-making and analysis, device O&M management, and service trend analysis.


This topic walks you through how to deliver integrated logs to LTS.

Prerequisites

- Logs you want to deliver have been aggregated in SecMaster. For details, see [Data Integration](#).
- To deliver data to LTS, ensure there is an available log group and log streams.

Procedure

Creating a Data Delivery

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Threat Operations > Security Analysis**. The security analysis page is displayed.
- 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**.
- 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.
- **Delivery Name:** Enter a data delivery name.
 - **Account Type:** Select **Current**. Only logs of the current account can be delivered to LTS.
 - **Delivery Type:** Select **LTS**.
 - **Log Group:** Select an LTS log group.
 - **Log Stream:** Select a destination LTS log stream.

Other configuration parameters are generated by the system by default and do not need to be configured.

- Step 8** Click **OK**.



Data Delivery Authorization

- Step 9** On the **Data Delivery** page, click the **Cross-Tenant Permissions** tab. On the page 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.

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.

Checking the Data Delivery Status

- Step 10** Click  in the upper left corner of the page and choose **Management & Governance > Log Tank Service**.
- Step 11** 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 the log group name.
- Step 12** Click the name of the log stream selected during data delivery. The log stream details page is displayed.

Step 13 On the log stream details page, view the delivered log information.

----End

10 Security Orchestration

10.1 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.

In security orchestration, playbooks and workflows are core elements. They are associated, dependent on each other, and work together to enable efficient security operations. **The following describes how they work together:**

- Definition:
 - **Playbook:** A playbook is a formal expression of the security operations process in the security orchestration system. It converts the security operations process and regulations into machine-read workflows.
Playbooks embody the logic of security protection controls and schedule security capabilities. Playbooks are flexible and scalable. They can be modified and extended based on actual requirements to adapt to ever-changing security threats and service requirements.
 - **A workflow** is a collaborative work mode that integrates various capabilities related to security operation, such as tools, technologies, workflows, and personnel. It consists of multiple connected components. After defined in a workflow, these components can be triggered externally. For example, when a new service ticket is generated, the automatic service ticket review workflow is automatically triggered. You can use the visual canvas to define component actions for each node in a workflow.
A workflow is a response mode when a playbook is triggered. Workflows convert instructions and procedures in the corresponding playbook into specific actions and execution steps.
- Relationships and differences
 - **Relationship:** A playbook provides guidance and rules for secure operations, and its workflow is responsible for converting these rules into

specific execution steps and actions. A playbook and its workflow depend on each other. The playbook guides the execution of the workflow, while the workflow implements the intent and requirements of the playbook.

- Differences: There are also some differences between playbooks and workflows. First, playbooks focus more on defining and describing security operation processes and regulations, so they focus on the overall framework and policies. Workflows focus more on specific actions and execution steps, so they focus on how to convert requirements in playbooks into actual actions. Second, playbooks are flexible and scalable, and can be modified and extended as required. However, workflows are relatively fixed. Once the design is complete, they need to follow the specified steps.

Example: Take a specific cyber security incident response case as an example. When an organization suffers from a network attack, the security orchestration system first identifies the attack type and severity based on the preset playbook. Then, the system automatically triggers corresponding security measures based on the workflow defined in the playbook, such as isolating the attacked system, collecting attack data, and notifying the security team. During the process, playbooks and workflows work closely to ensure the accuracy and timeliness of security responses.

10.2 Built-in Playbooks

In security orchestration module, SecMaster provides built-in playbooks. You can use them without extra settings.

Built-in Playbooks

Table 10-1 Built-in Playbooks

Security Layer	Playbook Name	Description	Data Class
Server security	HSS alert synchronization	Automatically synchronizes HSS alerts generated for servers.	Alert
	Auto High-Risk Vulnerability Notification	Sends email or SMS notifications to specified recipients when vulnerabilities rated as high severity are discovered.	Vulnerability
	Attack Link Analysis Alert Notification	Analyzes attack links. If HSS generates an alert for a server, the system checks the website running on the server. If the website information and alert exist, the system sends an alert notification.	Alert
	Server vulnerability notification	Checks servers with EIPs bound on the resource manager page and notifies of discovered vulnerabilities.	CommonContext

Security Layer	Playbook Name	Description	Data Class
	HSS Isolation and Killing of Malware	Automatically isolates and kills malware.	Alert
	Mining host isolation	Isolates the server for which an alert of mining program or software was generated. The playbook also adds the server into a security group that allows no inbound or outbound traffic.	Alert
	Ransomware host isolation	Isolates the server for which an alert of ransomware was generated. The playbook also adds the server into a security group that allows no inbound or outbound traffic.	Alert
	Host Defense Alarms Are Associated With Historical Handling Information	Associates new HSS alerts with HSS alerts handled earlier and adds historical handling details to the comment area for the corresponding HSS alerts.	Alert
	Add host asset protection status notification	Checks new servers and notifies you of servers unprotected by HSS.	Resource
	HSS High-Risk Alarm Interception Notification	Checks HSS high-risk alarms and generates to-do task notifications for source IP addresses that are not blocked by security groups. The to-do tasks will be reviewed manually. Once confirmed, the source IP addresses will be added to VPC block policy in SecMaster.	Alert
	Automated handling of host Rootkit event attacks	If a Rootkit alert is generated, this playbook automatically isolates the affected host by adding it to a security group that blocks all inbound and outbound traffic, and closes the alert.	Alert
	Automated handling of host rebound Shell attacks	If a reverse shell alert is generated, this playbook automatically isolates the affected host by adding it to a security group that blocks all inbound and outbound traffic, and closes the alert.	Alert
Application security	SecMaster WAF Address Group Association Policy	Associates SecMaster and WAF blacklist address groups for all enterprise projects.	CommonContext

Security Layer	Playbook Name	Description	Data Class
	WAF clear Non-domain Policy	Checks WAF protection policies at 09:00 every Monday and deletes policies with no rules included.	CommonContext
	Application Defense Alarms Are Associated With Historical Handling Information	Associates new WAF alerts with WAF alerts handled earlier and adds historical handling details to the comment area for the new alerts.	Alert
	Web login burst interception	Checks IP addresses that establish brute-force login connections. If the IP addresses are not whitelisted, the workflow generate a to-do task. The do-to task will be reviewed manually. Once it is confirmed that the IP addresses should be blocked, the IP addresses will be added to a WAF block policy in SecMaster.	Alert
O&M security	Real-time Notification of Critical Organization and Management Operations	Sends real-time notifications for O&M alerts generated by models. Currently, SMN notifications can be sent for three key O&M operations: attaching NICs, creating VPC peering connections, and binding EIPs to resources.	Alert
Identity security	Identity Defense Alarms Are Associated With Historical Handling Information	Associates new IAM alerts with IAM alerts handled earlier and adds historical handling details to the comment area for the new alerts.	Alert
Network security	Network Defense Alarms Are Associated With Historical Handling Information	Associates new CFW alerts with CFW alerts handled earlier and adds historical handling details to the comment area for new alerts.	Alert
Others/General	Automatic Notification of High-Risk Alerts	Sends email or SMS notifications when there are alerts rated as High or Fatal.	Alert
	Alert metric extraction	Extracts IP addresses from alerts, checks the IP addresses against the intelligence system, sets alert indicators for confirmed malicious IP addresses, and associates the indicators with the source alerts.	Alert

Security Layer	Playbook Name	Description	Data Class
	Automatic Disabling of Repeated Alerts	Closes the status of duplicate alerts when they are generated next time for the last 7 days and associates the alerts with the same name for the last 7 days.	Alert
	Automatic renaming of alert names	Generates custom alert names by combining specified key fields.	Alert
	Alert IP metric labeling	Adds attack source IP address and attacked IP address labels for alerts.	Alert
	IP intelligence association	Associates alerts with SecMaster intelligence (preferred) and ThreatBook intelligence.	Alert
	Asset Protection Status Statistics Notification	Collects statistics on asset protection status every week and sends notifications to customers by email or SMS.	CommonContext
	Alert statistics Notify	At 19:00 every day, collects statistics on alerts that are not cleared and sends notifications to customers by email or SMS.	Alert
	Auto Blocking for High-risk Alerts	If a source IP address launched more than three attacks, triggered high-risk or critical alerts, and hit the malicious label in ThreatBook, this playbook triggers the corresponding security policies in WAF, VPC, CFW, or IAM to block the IP address.	Alert
	Automatic clearing of low-risk alerts	This playbook automatically clear low-risk and informative alerts.	Alert

10.3 Security Orchestration Process

This topic describes how Security Orchestration works.

Figure 10-1 Security Orchestration process

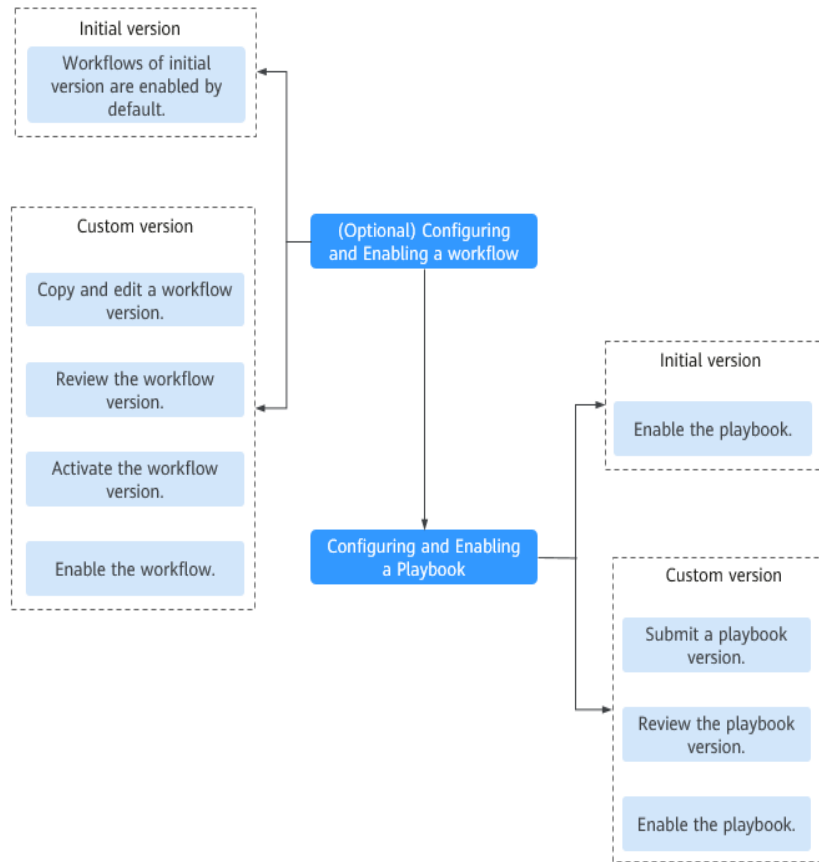


Table 10-2 Process

No.	Operation	Description
1	(Optional) Configuring and Enabling a Workflow	Enable the required workflows built in SecMaster. SecMaster provides some built-in workflows such as WAF uncapping, Synchronization of HSS alert status, and Fetching indicator from alert. Their initial version (V1) has been activated by default. If you need to edit a workflow, you can copy the initial version and edit it.
2	(Optional) Configuring and Enabling a Playbook	Enable the required playbooks built in SecMaster. By default, SecMaster provides playbooks such as Fetching indicator from alert, Synchronization of HSS alert status, and Automatic closing of repeated alerts. The initial version (V1) of the playbooks has been activated. You only need to enable them. If you need to edit a playbook, you can copy the initial version and edit it.

10.4 (Optional) Configuring and Enabling a Workflow


Scenario

SecMaster provides some built-in workflows such as WAF uncapping, Synchronization of HSS alert status, and Fetching indicator from alert. Their initial version (V1) has been activated by default.

You can customize and edit existing workflows. This topic describes how to configure and enable custom workflows.

Enabling a Workflow of a Custom Version

Accessing the workflow management page

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. Click **Workflows**.

Copying a workflow version

- Step 5** In the **Operation** column of the target workflow, click **More** and select **Version Management**.
- Step 6** On the **Version Management** slide-out panel for the workflow, in the **Version Information** area, locate the row containing the target workflow version, and click **Clone** in the **Operation** column.
- Step 7** In the displayed dialog box, click **OK**.

Editing and submitting a workflow version

- Step 8** On the **Version Management** slide-out panel for the workflow, in the **Version Information** area, locate the row containing the target workflow version, and click **Edit** in the **Operation** column.
- Step 9** 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 10-3 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.

Parameter		Description	
	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 10-4 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 10-4 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

Parameter	Description
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 .
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 10 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 11 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.

Step 12 On the **Version Management** slide-out panel for the workflow, click **Review** in the **Operation** column of the target workflow.

Step 13 In the displayed dialog box, set **Comment** to **Passed** and click **OK**.

Activating a workflow version

Step 14 On the **Version Management** slide-out panel for the workflow, in the **Version Information** area, locate the row containing the target workflow version, and click **Activate** in the **Operation** column.

Step 15 In the displayed dialog box, click **OK**.

Enabling a workflow

Some workflows have been enabled by default. You can enable other ones based on your needs. The procedure is as follows:

Step 16 On the **Version Management** slide-out panel, click **Enable** in the **Operation** column of the target workflow.

Step 17 On the slide-out panel displayed, select the workflow version to be enabled and click **OK**.

----End

10.5 Configuring and Enabling a Playbook

By default, SecMaster provides playbooks such as Fetching indicator from alert, Synchronization of HSS alert status, and Automatic closing of repeated alerts. The initial version (V1) of the playbooks has been activated. You only need to enable them.


If you need to edit a playbook, you can copy the initial version and edit it.

This section describes how to configure and enable a playbook.

- [Enabling a Playbook of the Initial Version](#)
- [Enabling a Playbook of a Custom Version](#)

Enabling a Playbook of the Initial Version

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**.

Step 5 In the **Operation** column of the target playbook, click **Enable**.


Step 6 Select the playbook version to be enabled and click **OK**.

----End

Enabling a Playbook of a Custom Version

Accessing the Playbook Version Management Page

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Security Orchestration > Playbooks**.

Copying a Playbook Version

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 **Clone** in the **Operation** column.

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

Editing and Submitting a Playbook Version

Step 7 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 8 On the page for editing a playbook version, edit the version information.

Step 9 Click **OK**.

Submitting a Playbook Version

Step 10 On the **Version Management** slide-out panel, in the **Version Information** area, locate the target playbook version, and click **Submit** in the **Operation** column.

Step 11 Click **OK**.

Reviewing a Playbook Version

Step 12 On the **Version Management** slide-out panel for the playbook, click **Review** in the **Operation** column of the target playbook.

Step 13 On the displayed page, set **Comment** to **Passed** and click **OK**.

Activating a Playbook Version

Step 14 On the **Version Management** slide-out panel, in the **Version Information** area, locate the row of the target playbook version, and click **Activate** in the **Operation** column.

Enabling a Playbook

Some playbooks have been enabled by default. You can enable other ones based on your needs. The procedure is as follows:

Step 15 On the **Playbooks** tab, locate the target playbook and click **Enable** in the **Operation** column.

Step 16 In the slide-out panel, select the playbook version you want to enable and click **OK**.

----End

10.6 Operation Object Management

10.6.1 Data Class

10.6.1.1 Viewing Data Classes


Scenario

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).

This section describes how to view existing data classes.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. The **Data Class** tab page is displayed by default.

Step 5 In the data class list, view the existing data class information.

- If there are many data classes displayed, use filters to search for a specific one.
- In the data class list, you can view the data class name, service code, and whether the data class is a built-in data class.
- 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.
On the data class details page, you can view the basic information and fields about the data class.

----End

10.6.2 Type Management

10.6.2.1 Managing Alert Types

Scenario


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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.
- Step 5** On the **Type Management** page, click the **Alert Type** tab.
- Step 6** On the **Alert 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 10-5](#).


If there are many subtypes, you can select the **Sub Type** or **Associated Layout** and enter the corresponding keyword for search.

Table 10-5 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

- Step 5** On the **Type Management** page, click the **Alert Type** tab.
- Step 6** On the **Alert Types** tab, click **Add**. On the **Add Alert Type** slide-out panel, set alert type parameters.

Table 10-6 Parameters for adding an alert type

Parameter	Description
Type Name	Customize the name of the new alert type.
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.
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.
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 **Alert Types** tab.

----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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

- Step 5** On the **Type Management** page, click the **Alert 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 target layout and 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.
- Step 5** On the **Type Management** page, click the **Alert Type** tab.
- Step 6** In the **Type Name** area on the **Alert Types** tab, 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 10-7 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.
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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Alert Type** tab.

Step 6 On the **Alert Types** tab, manage alert types.

NOTE

- The built-in alert types are enabled by default. You do not need to manually enable them.
- Currently, built-in alert types cannot be disabled or deleted.
- Currently, built-in alert types cannot be deleted.

Table 10-8 Managing an alert type

Operation	Description
Enable	<ol style="list-style-type: none"> 1. On the Alert Types tab, select the types you want to enable and click Batch enable. Alternatively, locate the row containing the alert type you want to enable, 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.
Disable	<ol style="list-style-type: none"> 1. On the Alert Types tab, select the types you want to disable and click Batch Disable. Alternatively, locate the row containing the alert type 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.
Delete	<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 displayed dialog box, click OK.

----End

10.6.2.2 Managing Incident Types

Scenario

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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Event Types** tab.

Step 6 On the **Event Types** tab, view the details about existing incident types. For details about the parameters, see [Table 10-9](#).

Table 10-9 Incident type parameters


Parameter	Description
Type Name	Name of an incident type

Parameter	Description
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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Event Types** tab.

Step 6 On the **Event Types** tab, click **Add**. On the **Add Event Type** slide-out panel, set incident type parameters.

Table 10-10 Incident type parameters

Parameter	Description
Type Name	Customized name of an incident type.
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.
Sub Type Tag	Enter the incident subtype ID. The keyword must comply with the upper camel case naming rules, for example, SubTypeName .
Startup Status	Indicates whether an incident type is enabled.
SLA	Set the SLA processing time of the incident.

Parameter	Description
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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Event Types** tab.

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 target layout and 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 part of the page and choose **Security > SecMaster**.

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

- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.
- Step 5** On the **Type Management** page, click the **Event Types** tab.
- 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 10-11 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.
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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.
- Step 5** On the **Type Management** page, click the **Event Types** tab.
- Step 6** On the incident type tab, manage incident types.

NOTE

- The built-in incident types are enabled by default. You do not need to manually enable them.
- Currently, built-in incident (event) types cannot be disabled or deleted.

Table 10-12 Managing existing incident types

Operation	Description
Enable	<ol style="list-style-type: none"> 1. 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. 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.
Disable	<ol style="list-style-type: none"> 1. 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. 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.
Delete	<ol style="list-style-type: none"> 1. On the incident type management page, select the type to be deleted and click Delete in the Operation column. 2. In the displayed dialog box, click OK.

----End

10.6.2.3 Managing Threat Intelligence Types

Scenario

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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

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 10-13](#).

Table 10-13 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.
- 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 10-14 Threat intelligence type parameters

Parameter	Description
Type Name	Name of the threat intelligence to be added.
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.
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 part of the page and choose **Security > SecMaster**.

- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
 - Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.
 - 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 **Associate Layout** dialog box, select the target layout and click **OK**.
- End

Editing a Threat Intelligence Type

 NOTE

- Currently, built-in threat intelligence types cannot be edited.
- After a custom threat intelligence type is added, the type tag cannot be edited.


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.
- 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 10-15 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:
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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Threat Intelligence** tab.

Step 6 On the threat intelligence type tab, manage threat intelligence types.

 **NOTE**

- Built-in threat intelligence types are enabled by default. You do not need to manually enable them.
- Currently, built-in threat intelligence types cannot be disabled or deleted.

Table 10-16 Managing a threat intelligence type

Operation	Description
Enable	<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.
Disable	<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.

Operation	Description
Delete	<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 displayed dialog box, click OK.

----End

10.6.2.4 Managing Vulnerability Types

Scenario

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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

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 10-17](#).

Table 10-17 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.
- 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 10-18 Vulnerability type parameters

Parameter	Description
Type Name	Name of the vulnerability type to be added.
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:
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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

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 **Associate Layout** dialog box, select the target layout and 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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

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 10-19 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:
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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Vulnerability Type** tab.

Step 6 On the vulnerability type tab, manage vulnerability types.

 **NOTE**

- Built-in vulnerability types are enabled by default. You do not need to manually enable them.
- Currently, the built-in vulnerability types cannot be disabled or deleted.

Table 10-20 Managing a vulnerability type

Operation	Description
Enable	<ol style="list-style-type: none"> 1. 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. 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.

Operation	Description
Disable	<ol style="list-style-type: none"> 1. 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. 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.
Delete	<ol style="list-style-type: none"> 1. On the Vulnerability Type tab, select the vulnerability type to be deleted and click Delete in the Operation column. 2. In the displayed dialog box, click OK.

----End

10.6.2.5 Managing Custom Types

Scenario

This section describes how to manage custom object types.

- **Adding a Custom Type**: describes how to define types.
- **Adding a Subtype for a User-Defined Type**: describes how to define subtypes.
- **Associating a Custom Type/Subtype with a Layout**: describes how to associate a user-defined type or subtype with an existing layout.
- **Editing a Custom Type/Subtype**: describes how to edit a user-defined type or subtype.
- **Enabling/Disabling a User-defined Subtype**: describes how to enable or disable a new type or subtype.
- **Viewing Custom Types or Subtypes**: describes how to view new user-defined types and subtypes.
- **Deleting a Custom Type or Subtype**: describes how to delete a user-defined type or subtype.

Limitations and Constraints

- Built-in types and sub-types cannot be associated with layouts, edited, deleted, enabled, or disabled.
- After a custom type is added, its values of **Data Class**, **Type Name**, and **Type ID** cannot be modified.
- After a subtype is added, its values of **Data Class**, **Type Name**, **Type ID**, and **Subtype ID** cannot be modified.

Adding a Custom Type


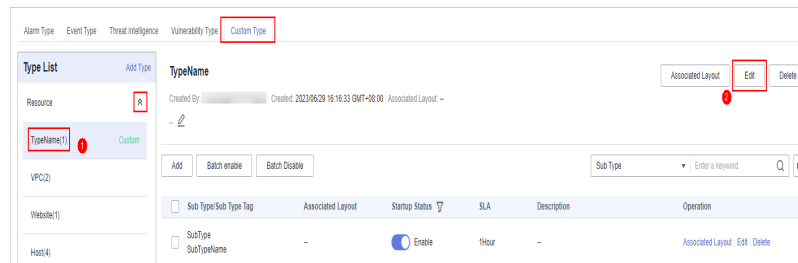
- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.
- Step 5** On the **Type Management** page, click the **Custom Type** tab. On the displayed page, click **Add**.

Figure 10-2 Add Type



- Step 6** On the **Add Type** page, set type parameters.

Table 10-21 User-defined type parameters

Parameter	Description
Data Class	Select an existing data class.
Type Name	Create a name for the type you want to define.
Type Tag	Enter a type tag. The keyword must comply with the upper camel case naming rules, for example, TypeTag .
Startup Status	The enabling status of the type:
Description	Description of a custom type.

 **NOTE**

After a user-defined type is added, the **Data Class**, **Type Name**, and **Type ID** cannot be modified.

- Step 7** In the lower right corner of the page, click **OK**.

After the type is added, you can view the new type in the **Type List** on the **User-Defined Types** page.

----End

Adding a Subtype for a User-Defined Type


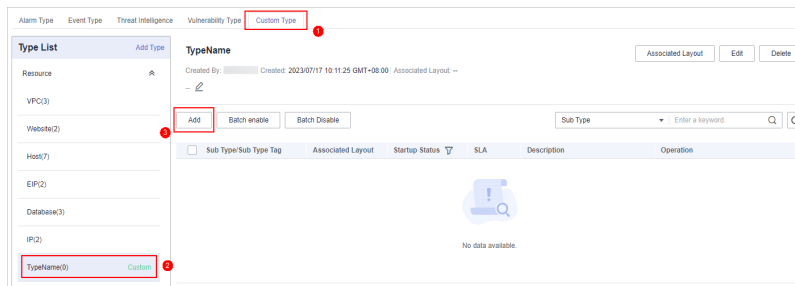
- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.
- Step 5** On the **Type Management** page, click the **Custom Type** tab. In the type list on the left, click the name of the custom type for which you want to add a subtype. Details about the custom type are displayed on the right.
- Step 6** On the **Custom Types** page on the right, click **Add**.

Figure 10-3 Adding a subtype



- Step 7** On the **Add Subtype** page, set parameters.

Table 10-22 Subtype parameters

Parameter	Description
Data Class	Name of the current data class.
Type Name	Name of the current type.
Type ID	ID of the current type.
Subtype	User-defined subtype keyword.
Subtype ID	Custom subtype ID. The keyword must comply with the upper camel case naming rules, for example, SubTypeTag .
Status	Indicates the enabling status of the subtype:
SLA	Set the SLA processing time of the subtype.
Description	Description of a subtype

- Step 8** Click **OK**.


----End

Associating a Custom Type/Subtype with a Layout

NOTE

Built-in types and subtypes have been associated with layouts by default. You cannot customize associated layouts.

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Custom Type** tab. On the displayed page, perform operations based on the type.

- For a **type**:
 - a. In the **Type List** on the left of the **Custom Type** page, select the type to be associated with a layout.
 - b. In the detailed information about the type on the right, click **Associate Layout**. The **Associate Layout** dialog box is displayed.
 - c. In the **Associate Layout** dialog box, select the target layout and click **OK**.
- For a **subtype**:
 - a. In the **Type List** on the left of the **Custom Type** page, select the type to be associated with a layout.
 - b. In the subtype list of this type displayed on the right, click **Associate Layout** in the **Operation** column of the target type to associate with the layout. The **Associate Layout** dialog box is displayed.
 - c. In the **Associate Layout** dialog box, select the target layout and click **OK**.


----End

Editing a Custom Type/Subtype

NOTE

- Built-in types and subtypes cannot be edited.
- After a user-defined type is added, the **Data Class**, **Type Name**, and **Type ID** cannot be modified.
- After a subtype is added, its **Data Class**, **Type Name**, **Type Tag**, **Sub Type**, and **Sub Type Tag** cannot be modified.

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Custom Type** tab. On the displayed page, perform operations based on the type.

- For a **type**:
 - a. In the **Type List** on the left of the **Custom Type** page, select the type to be edited.
 - b. Click **Edit** on the target type detail page. The **Edit Type** page is displayed on the right.
 - c. On the **Edit Type** page, edit the parameters of the type.

Table 10-23 Type parameters

Parameter	Description
Data Class	Data class to which the type belongs, which cannot be modified.
Type Name	Name of a user-defined type, which cannot be modified.
Type ID	Vulnerability type ID, which cannot be modified.
Status	The enabling status of the type.
Description	Description of a custom type

- d. In the lower right corner of the page, click **Confirm**.
- For a **subtype**:
 - a. In the **Type List** on the left of the **Custom Type** page, select the type you want to edit.
 - b. In the subtype list of this type on the right, click **Edit** in the **Operation** column of the target subtype. The **Edit Subtype** page is displayed on the right.
 - c. On the **Edit Subtype** page, edit the parameters of the subtype.

Table 10-24 Subtype parameters

Parameter	Description
Data Class	Data class to which the type belongs, which cannot be modified.
Type Name	Name of a user-defined type, which cannot be modified.
Type ID	Vulnerability type ID, which cannot be modified.
Subtype Name	Name of the sub type, which cannot be edited.
Subtype ID	Subtype ID, which cannot be modified.
Startup Status	The enabling status of the subtype.

Parameter	Description
SLA	SLA processing time of the subtype
Description	Description of a custom subtype

- d. In the lower right corner of the page, click **OK**.


----End

Enabling/Disabling a User-defined Subtype

NOTE

Built-in subtypes are enabled by default and cannot be disabled.

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Custom Type** tab. In the type list on the left of the page, select the type you want to associate with the layout.

Step 6 In the subtype list displayed on the right, enable or disable the target subtype in the **Startup Status** column.

You can batch enable or disable subtypes. To do so, select them and click **Batch enable** or **Batch Disable** in the upper left corner above the type list.


Step 7 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 **Disabled** (or **Enabled**), the target type is disabled (or enabled).

----End

Viewing Custom Types or Subtypes

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Custom Type** tab. On the displayed page, view details about existing custom types or subtypes.

- The type list is displayed on the left, showing the existing types.
- To view details about a type, click the type name in the type list. The type details are displayed on the right. The detailed information is as follows:
 - Basic information about the target type: name, creator, creation time, and associated layout.
 - Subtype list: information about existing subtypes, subtype names, and layouts associated with subtypes.


----End

Deleting a Custom Type or Subtype

NOTE

Built-in types and subtypes cannot be deleted.

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the displayed page, click the **Type Management** tab.

Step 5 On the **Type Management** page, click the **Custom Type** tab. On the displayed page, perform operations based on the type.

- For a type:
 - a. In the **Type List** on the left of the **Custom Type** page, select the target.
 - b. In the right pane, click **Delete** on the target type page to delete the type. A dialog box is displayed for you to confirm the deletion.
 - c. In the displayed dialog box, click **OK**.
- For a subtype:
 - a. In the **Type List** on the left of the **Custom Type** page, select the target type.
 - b. In the subtype list of this type on the right, click **Delete** in the **Operation** column of the target type to be deleted. The deletion confirmation dialog box is displayed.
 - c. In the displayed dialog box, click **OK**.

----End

10.6.3 Classification & Mapping


10.6.3.1 Viewing Categorical Mappings

Scenario

Categorical mappings are used to match alert types and map alert fields for aloud service alerts.

This section describes how to view categorical mappings.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.
- Step 5** On the **Classify&Mapping** tab, view details about the created categorical mappings.
 - In the categorical mapping list, view details such as the categorical mapping name, data class, and number of associated plug-in instances.
 - If there are so many categorical mappings, you can use filters and keywords to search for a specific one.
 - To edit a categorical mapping, click its name to go to the edit page. On the edit page, you can edit details about the categorical mapping.
 - In the categorical mapping list, you can also enable, disable, clone, and delete a categorical mapping.

----End

10.6.3.2 Creating, Copying, and Editing a Categorical Mapping

Scenario

Classification and mapping are to perform class matching and field mapping for cloud service alerts.

This section walks you through on how to create, edit, and copy a classification and mapping.

Creating a Categorical Mapping





- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.
- Step 5** On the **Classify&Mapping** page, click **Create**.
- Step 6** On the **Create Categorical Mapping** page, set categorical mapping parameters.
 1. In the **Basic Parameters** area on the left, configure basic information about the categorical mapping. For details about the parameters, see [Table 10-25](#).

Table 10-25 Configuring basic information


Parameter	Description
Name	Name of a user-defined categorical 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 categorical 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 categorical mapping is complete, click  at the upper right corner of the page to save the configuration.
7. On the **Preprocessing** tab on the right, set preprocessing mapping parameters.
8. Click  at the upper right corner of the page to save the configuration.

----End

Copying a Categorical Mapping

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.

Step 5 On the **Classify&Mapping** page, click **Clone** in the **Operation** column of the target categorical mapping.

Step 6 In the displayed dialog box, enter the name for replicated mapping and click **OK**.

----End

Editing a Categorical Mapping

Step 1 Log in to the management console.





- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.
- Step 5** On the **Classify&Mapping** page, click the target categorical mapping name to go to the edit page.
- Step 6** On the **Edit Categorical Mapping** page, set parameters.
 1. In the **Basic Parameters** area on the left, configure basic information about the categorical mapping. For details about the parameters, see [Table 10-25](#).

Table 10-26 Configuring basic information

Parameter	Description
Name	Name of a user-defined categorical mapping.
Data Category	This field cannot be edited.
Description	Description of the custom categorical mapping.

2. In the **Data Source** area on the left, select the data source for the categorical mapping.
If **Data Source** is set to **Upload JSON file**, you need to click **Upload JSON file** and upload the JSON file.
 3. On the **Classify** tab 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 on the right, select a mapping mode and set related parameters.
 6. After the categorical mapping is complete, click  at the upper right corner of the page to save the configuration.
 7. On the **Preprocessing** tab on the right, set preprocessing mapping parameters.
 8. Click  at the upper right corner of the page to save the configuration.
- End


10.6.3.3 Managing Categorical Mappings

Scenario

This topic describes how to manage categorical mappings, such as enabling, disabling, and deleting a categorical mapping.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Objects**. On the page displayed, click the **Classify&Mapping** tab.

Step 5 On the **Classify&Mapping** tab, manage categorical mappings.

 **NOTE**

- Custom categorical mappings cannot be enabled or disabled.
- Currently, built-in categorical mappings cannot be deleted.

Table 10-27 Managing categorical mappings

Operation	Description
Enable	Locate the row containing the target categorical mapping and click Disable in the Status column. If the status changes to Enable , the categorical mapping has been enabled.
Disable	Locate the row containing your desired categorical mapping and click Enable in the Status column. If the status changes to Disable , the categorical mapping has been disabled.
Delete	<ol style="list-style-type: none"> 1. Click Delete in the Operation column of the target categorical mapping. 2. In the displayed pane on the right, click Delete. <p>NOTE</p> <ul style="list-style-type: none"> - If a categorical mapping is deleted, the plug-ins and connections associated with it will be stopped immediately. - Deleted categorical mappings cannot be restored. Exercise caution when performing this operation.

----End

10.7 Playbook Orchestration Management

10.7.1 Playbooks

10.7.1.1 Submitting a Playbook Version

Scenario


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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**.

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 **Pending review**.
- 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](#).

10.7.1.2 Reviewing a Playbook Version

Scenario

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**.
- 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 10-28](#) describes the parameters for reviewing a playbook version.

Table 10-28 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](#).

10.7.1.3 Enabling a Playbook


Scenario

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 part of the page and choose **Security > SecMaster**.
 - Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
 - Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**.
 - Step 5** In the **Operation** column of the target playbook, click **Enable**.
 - Step 6** Select the playbook version you want to enable and click **OK**.
- End

10.7.1.4 Managing Playbooks

Scenario


This section describes how to manage playbooks, including [Viewing Existing 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**.
- Step 5** On the **Playbooks** tab page, view playbook information.
 - The numbers of **Pending review**, **Not enabled**, and **Enabled** playbooks are displayed above the playbook list.
 - View the information about existing playbooks.
If there are many playbooks displayed, use filters to search for a specific one.

To view details about a playbook, click its name to go to its details page.

Table 10-29 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
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

----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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**.
- 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**.
- 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**.

Step 5 In the **Operation** column of the playbook to be deleted, click **Delete**.

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

 **NOTE**

Deleting a playbook will delete all its versions by default. Deleted playbook versions cannot be restored. Exercise caution when performing this operation.

----End

10.7.1.5 Managing Playbook Versions

Scenario


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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**.

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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**.
- 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 **Edit** in the **Operation** column.
- Step 7** On the page for editing a playbook version, edit the version information.
- Step 8** 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**.
- 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.

Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**.

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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**.

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

10.7.2 Workflows


10.7.2.1 Reviewing a Workflow Version

Scenario

This topic describes how to review a workflow version.

Procedure

Step 1 Log in to the management console.

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

- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. Click **Workflows**.
- Step 5** In the **Operation** column of the target workflow, click **More** and select **Version Management**.
- Step 6** On the **Version Management** slide-out panel, click **Review** in the **Operation** column of the target workflow.
- Step 7** Set **Comments**. [Table 10-30](#) describes the parameters.

Table 10-30 Workflow review parameters

Parameter	Description
Comment	Select the review conclusion. <ul style="list-style-type: none"> • Approved: If the workflow version is approved, the status of the workflow version changes to Activated. • Rejected. If 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](#).

10.7.2.2 Enabling a Workflow


Scenario

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 part of the page and choose **Security > SecMaster**.
 - Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
 - Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. Click **Workflows**.
 - Step 5** In the row containing the target workflow, click **Enable** in the **Operation** column.
 - Step 6** In the slide-out panel that is displayed, select the workflow version to be enabled and click **OK**.
- End

10.7.2.3 Managing Workflows

Scenario

This section describes how to manage workflows, including [Viewing Workflows](#), [Exporting Workflows](#), [Deleting Workflows](#), and [Disabling a Workflow](#).

Viewing Workflows


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. Click **Workflows**.
- Step 5** On the **Workflows** page, view details about the created workflow.

Figure 10-4 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 many workflows displayed, use filters to search for a specific one.

Table 10-31 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.

- To view details about a workflow, click its name to access its details page.


----End

Exporting Workflows

NOTE


Workflows in the **Enabled** state can be exported.

Step 1 Log in to the management console.

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

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

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

Step 5 On the **Workflows** tab page, select the workflows to be exported and click  in the upper right corner of the list.

Step 6 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 Log in to the management console.

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

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

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

Step 5 On the **Workflows** tab page, locate the row containing the target workflow and click **Delete** in the **Operation** column.

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


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 Log in to the management console.


- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. Click **Workflows**.
- Step 5** In the row containing the target workflow, click **Disable** in the **Operation** column.
- Step 6** In the dialog box that is displayed, click **OK**.
- End

10.7.2.4 Managing Workflow Versions

Scenario

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** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. Click **Workflows**.
- Step 5** In the **Operation** column of the target workflow, click **More** and select **Version Management**.
- Step 6** 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 7** 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** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.

- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. Click **Workflows**.
- Step 5** In the **Operation** column of the target workflow, click **More** and select **Version Management**.
- Step 6** 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 7** 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 10-32 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 10-33 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.)

Parameter			Description
		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 10-33 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 .
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 8 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 Log in to the management console.

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

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

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

Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Step 6 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.

Step 7 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 Log in to the management console.

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

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

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

Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.


Step 6 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.

Step 7 In the dialog box that is displayed, click **OK**.

----End

Deleting a Workflow Version

Step 1 Log in to the management console.

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

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

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

Step 5 In the **Operation** column of the target workflow, click **More** and select **Version Management**.

Step 6 On the **Version Management** slide-out panel, in the version information area, locate the row of the target workflow version, and click **Delete** in the **Operation** column.

Step 7 In the displayed dialog box, click **OK**.

NOTE

Deleted workflow versions cannot be retrieved. Exercise caution when performing this operation.

----End

10.7.3 Asset Connections

10.7.3.1 Adding an Asset Connection

Scenario

- **Concept:** An asset connection includes the domain name and authentication parameters required by each plug-in node in the security orchestration process.
- **Function:** During security orchestration, each plug-in node transfers the domain name to be connected and the authentication information, such as the username, password, and account AK/SK, to establish connections.
- **Relationship between asset connections and plug-ins:** Plug-ins access other cloud services or third-party services through domain names and authentication. So, domain name parameters (endpoints) and authentication parameters (username/password, account AK/SK, etc.) are defined in the login credential parameters of plug-ins. An asset connection configures login credential parameters for a plug-in. In a workflow, each plug-in node is

associated with different asset connections so that the plug-in can access different services.

This topic describes how to create an asset.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. On the displayed page, click the **Asset Connections** tab.
- 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 10-34](#).

Table 10-34 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 .

Parameter	Description
Connection Type	<p>Select the type of the asset connection.</p> <ul style="list-style-type: none"> • Cloud service agency: When a cloud service plug-in is used, you are advised to use the cloud service agency. You do not need to manually enter authentication parameters such as the domain name, username, and password. The system automatically obtains the domain name (endpoint) of the corresponding cloud service based on the plug-in name and uses the cloud service agency for authentication. • AK&SK: You need to manually enter the domain name (endpoint) and provide an AK and SK for authentication. • Username and password: You need to manually enter the domain name (endpoint) and provide a username and password for authentication. • Others: Some plug-ins have other authentication parameters in addition to the preceding authentication parameters. Set these parameters based on the plug-in login credential parameter guide.
Credential	Enter the credential information, such as the endpoint, AK, and SK, based on the selected connection type.

Step 7 Click **OK**. You can query the created asset connection in the asset connection list.

----End


10.7.3.2 Managing Asset Connections

Scenario

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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**. On the displayed page, click the **Asset Connections** tab.

Step 5 On the **Asset connection** tab page, view information about existing asset connections.

Figure 10-5 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 OMT...	--	--	Alert handling method set	Edit Delete
VPC authentication	ACL	system	2023/09/24 14:35:52 OMT...	--	--	VPC authentication	Edit Delete
SMN notification to...	HTTP	system	2023/09/24 14:35:52 OMT...	--	--	SMN notification token for operat...	Edit Delete
SecMaster authent...	HTTP	system	2023/09/24 14:35:52 OMT...	--	--	SecMaster authentication token	Edit Delete
CFW authentication...	HTTP	system	2023/09/24 14:35:52 OMT...	--	--	CFW authentication token	Edit Delete
SMN notification to...	HTTP	system	2023/09/24 14:35:52 OMT...	--	--	SMN notification token for handli...	Edit Delete
WAF authentication...	HTTP	system	2023/09/24 14:35:52 OMT...	--	--	WAF authentication token	Edit Delete
DBSS authentication...	DBSS	system	2023/09/24 14:35:52 OMT...	--	2023/04/13 22:28:25 OMT...	DBSS authentication token	Edit Delete
HSS authentication ...	HSS	system	2023/09/24 14:35:52 OMT...	--	--	HSS authentication token	Edit Delete
ECS authentication ...	ECS	system	2023/09/24 14:35:52 OMT...	--	--	ECS authentication token	Edit Delete

- In the asset connection list, you can view the name, plug-in, and creator of an asset connection.
- If there are many asset connections displayed, use filters to search for a specific one.
- To view details about an asset connection, click its name to go to its **Detail** panel.

----End

Editing an Asset Connection


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. On the displayed page, click the **Asset Connections** tab.
- 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 10-35](#).

Table 10-35 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.


Parameter	Description
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 .
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 .
Connection Type	Select the type of the asset connection.
Credential	Enter the credential information, such as AK and SK, based on the selected connection type.

Step 7 Click **OK**.

----End

Deleting an Asset Connection

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Playbooks**. On the displayed page, click the **Asset Connections** tab.

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

10.7.4 Instance Management

10.7.4.1 Viewing Monitored Playbook Instances

Scenario

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.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Playbooks**. On the displayed page, click the **Instance Management** tab.
- Step 5** On the **Instance Management** tab, click the **Playbook Instances** or **Workflow Instances** tab, and view the instance information. For details about the parameters, see [Table 10-36](#).
 - You can view the total number of instances below the instance list. You can view a maximum of 10,000 instance records page by page. To view more than 10,000 records, optimize the filter criteria.
 - An instance can be stored for a maximum of 180 days.
 - To view details about an instance, click the instance name. On the displayed page, you can view the instance workflow, workflow nodes, start time, and end time.

Table 10-36 Parameters in the instance list

Parameter	Description
Instance Name	Name of the instance generated by the system.
Playbook/ Instance Name	Name of the playbook/instance corresponding to the instance.
Data Class	Operation object of a playbook
Trigger Method	Triggering mode of an instance <ul style="list-style-type: none"> • Timer Trigger • Event Trigger

Parameter	Description
Status	<p>Status of an instance</p> <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 Ended	Time when an instance ends.
Operation	You can terminate or retry an instance.

----End

Related Operations

- To stop a running instance, click **Terminate** in the **Operation** column of the target instance. After an instance is terminated, no operations are supported.
- To start a failed instance, click **Retry** in the **Operation** column.
You can retry instances up to 100 times a day in a single workspace. After a retry, the playbook cannot be retried until the current execution is complete.

10.8 Layout Management

10.8.1 Viewing an Existing Layout Template


Scenario

There are many management page and details page templates, for example, alert, incident, and vulnerability management templates.

This section describes how to learn what types of layout templates you can have.

Procedure

- Step 1** Log in to the management console.


- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Layouts**. On the displayed page, click the **Template** tab.
- Step 5** On the **Template** tab, 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 a template.
 - You can edit the name and layout of a template.
- End


10.8.2 Manage Existing Layouts

Scenario

This topic describes how to view and delete layouts.

Viewing an Existing Layout


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Layouts**.
- 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

Custom page layouts can be deleted.

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Security Orchestration > Layouts**.

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

10.9 Plug-in Management

10.9.1 Plug-in Management 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.


10.9.2 Viewing Plug-in Details

Scenario

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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation pane on the left, choose **Security Orchestration > Plugins**.

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

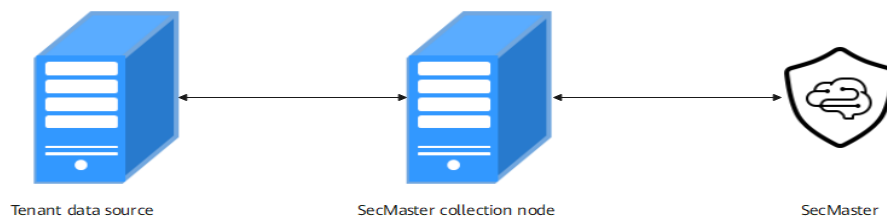
11 Settings

11.1 Data Collection

11.1.1 Data Collection Overview

You can enable access to third-party logs in SecMaster. SecMaster uses Logstash to collect logs from many types of sources. Logs are comprehensively collected for historical data analysis, associated data analysis, and unknown threat detection.

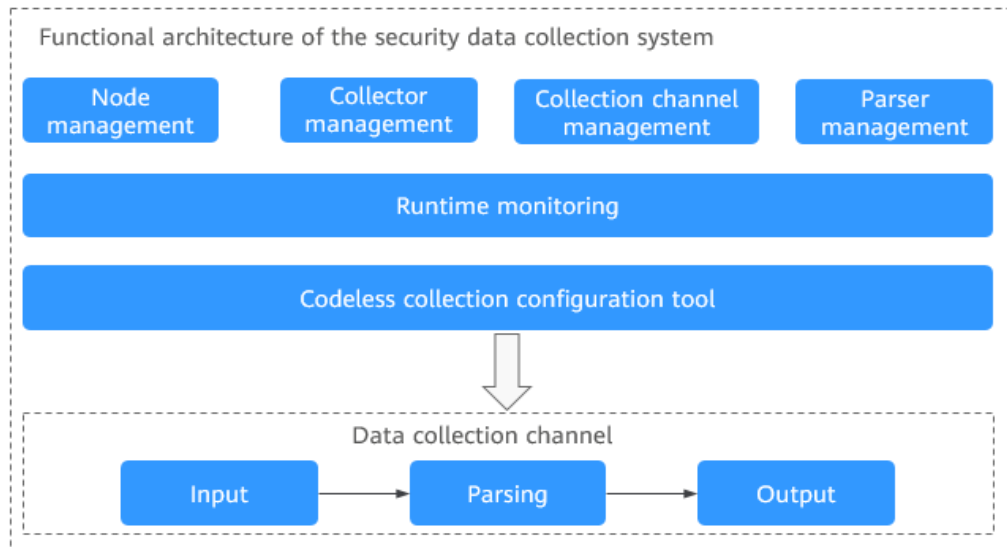
Figure 11-1 Data Collection



Data Collection Principles

The basic principle of data collection is as follows: SecMaster uses a component controller (isap-agent) that is installed on your ECSs to manage the collection component Logstash, and Logstash transfer security data in your organization or between you and SecMaster.

Figure 11-2 Functional architecture of the collection system



Description

- Collector: custom Logstash. A collector node is a custom combination of Logstash+ component controller (isap-agent).
- Node: If you install SecMaster component controller isap-agent on an ECS, the ECS is called a node. You need to deliver data collection engine Logstash to managed nodes on the **Components** page.
- Component: A component is a custom Logstash that works as a data aggregation engine to receive and send security log data.
- Connector: A connector is a basic element for Logstash. It defines the way Logstash receives source data and the standards it follows during the process. Each connector has a source end and a destination end. Source ends and destination ends are used for data inputs and outputs, respectively. The SecMaster pipeline is used for log data transmission between SecMaster and your devices.
- Parser: A parser is a basic element for configuring custom Logstash. Parsers mainly work as filters in Logstash. SecMaster preconfigures varied types of filters and provides them as parsers. In just a few clicks on the SecMaster console, you can use parsers to generate native scripts to set complex filters for Logstash. In doing this, you can convert raw logs into the format you need.
- Collection channel: A collection channel is equivalent to a Logstash pipeline. Multiple pipelines can be configured in Logstash. Each pipeline consists of the input, filter, and output parts. Pipelines work independently and do not affect each other. You can deploy a pipeline for multiple nodes. A pipeline is considered one collection channel no matter how many nodes it is configured for.

Limitations and Constraints

- Currently, the data collection component controller can run on ECSs running the Linux x86_64 or Arm64 architecture.

Collector Specifications

The following table describes the specifications of the ECSs that are selected as nodes in collection management.

Table 11-1 Collector Specifications

vCPUs	Memory	System Disk	Data Disk	Referenced Processing Capability
4 vCPUs	8 GiB	50 GiB	100 GiB	2,000 EPS @ 1 KB 4,000 EPS @ 500 B
8 vCPUs	16 GiB	50 GiB	100 GiB	5,000 EPS @ 1 KB 10,000 EPS @ 500 B
16 vCPUs	32 GiB	50 GiB	100 GiB	10,000 EPS @ 1 KB 20,000 EPS @ 500 B
32 vCPUs	64 GiB	50 GiB	100 GiB	20,000 EPS @ 1 KB 40,000 EPS @ 500 B
64 vCPUs	128 GiB	50 GiB	100 GiB	40,000 EPS @ 1 KB 80,000 EPS @ 500 B
<p>NOTE</p> <p>The ECS must have at least two vCPUs and 4 GB of memory. A disk of at least 100 GB must be attached as the directory disk.</p> <p>The log volume usually increases in proportion to the server specifications. Generally, you are advised to increase the log volume based on the specifications in the table. If there is huge pressure on a collector, you can deploy multiple collectors and manage them in a unified manner through collection channels. This can distribute the log forwarding pressure across collectors.</p> <p>Before installing the component controller, you are advised to mount a disk and use the disk partitioning script to allocate the disk. To ensure the installation and running of Logstash, the directory partition must have more than 100 GB of free space.</p>				

Log Source Limit

You can add as many as log sources you need to the collectors as long as your cloud resources can accommodate those logs. You can scale cloud resources anytime to meet your needs.

Data Collection Process

Figure 11-3 Data collection process

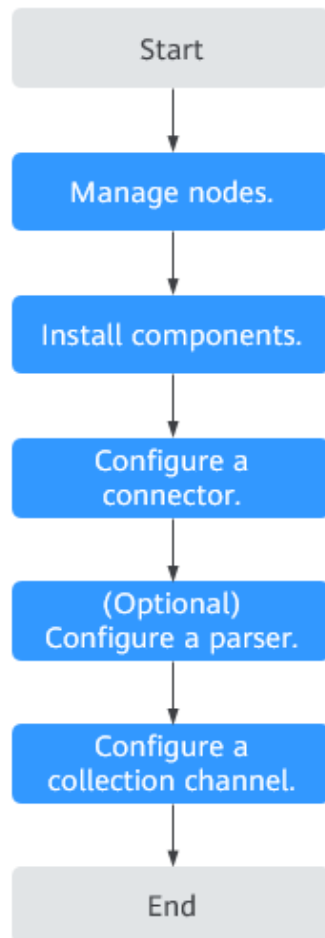


Table 11-2 Description of the data collection process

No.	Step	Description
1	Managing Nodes	Select or purchase an ECS and install the component controller on the ECS to complete node management.
2	Installing Components	Install data collection engine Logstash on the Components tab to complete component installation.
3	Configuring Connectors	Configure the source and destination connectors. Select a connector as required and set parameters.
4	(Optional) Configuring a Parser	Configure codeless parsers on the console based on your needs.

No.	Step	Description
5	Configuring a Collection Channel	Configure the connection channels, associate it with a node, and deliver the Logstash pipeline configuration to complete the data collection configuration.
6	Verifying the Collection Result	After the collection channel is configured, check whether data is collected. If logs are sent to the SecMaster pipeline, you can query the result on the SecMaster Security Analysis page.

Data Collection Configuration Removal Process

Figure 11-4 Data collection configuration removal process

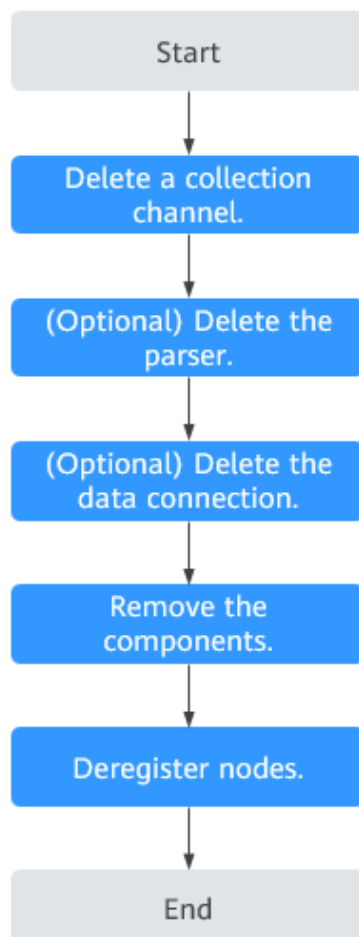


Table 11-3 Description of the data collection configuration removal process

No.	Step	Description
1	Deleting a collection channel	On the Collection Channels page, stop and delete the Logstash pipeline configuration. Note: All collection channels on related nodes must be stopped and deleted first.
2	(Optional) Deleting a parser	If a parser is configured, delete it on the Parsers tab.
3	(Optional) Deleting a data connection	If a data connection is added, delete the source and destination connectors on the Connections tab.
4	Removing a component	Delete the collection engine Logstash installed on the node and remove the component.
5	Deregistering a node	Remove the component controller to complete node deregistration. Note: Deregistering a node does not delete the ECS and endpoint resources. If the data collection function is no longer used, you need to manually release the resources.

11.1.2 Component Management

11.1.2.1 Creating and Editing a Node

Scenario

This topic describes how to create and edit a data collection node.

 **CAUTION**

The recommended installation path is **/opt/cloud**. This section also uses this path as an example. You can use other installation paths. Make sure change the path when you refer to the example here. For example, if the installation path is **/tmp**, change the installation path in this section to **/tmp**.

Preparations

- **Checking the disk space**

Check the disk space in the **/opt** directory of the ECS where you will install the component controller and make sure the space is not smaller than 100 GB.

- a. Remotely log in to the ECS where you want to install the component controller.

- 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 component controller on the server as user **root**.
- b. Run the **df -h** command to check whether more than 100 GB space is reserved in the **/opt** directory of the disk. At least 2 vCPUs and 4 GB of memory are required.



Figure 11-5 Checking 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.

To ensure that the **/opt** directory has more than 100 GB free disk space allocated, you can use the disk partitioning script to allocate the disk. For details, see [Partitioning a Disk](#).

Creating a Node

- Step 1** Check operations in [Preparations](#) and log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Components**.
- Step 5** On the **Nodes** tab, click **Create**. The **Create Node** page is displayed on the right.
- Step 6** On the **Create Node** page, configure a channel.
1. In the **Network Channel Settings** area, select the VPC and subnet the target ECS belongs to.
 2. In the network channel list, click **Config** in the **Operation** column of each channel. In the displayed confirmation dialog box, click **Confirm**.
- Step 7** Click **Next** in the lower right corner of the page to go to the **Script Installation Verification** page.
- Step 8** Select the ECS OS, follow the step, and click  to copy the command for installing the component controller.


- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Components**.
- Step 5** On the **Nodes** tab, locate the row that contains the target node and click **Edit** in the **Operation** column.
- Step 6** On the **Edit Node** panel, edit the node information.

Table 11-4 Parameters of node information

Parameter	Description
Data Center	User-defined data center name
Network Plane	Select the network plane of the node.
Tag	Set the tag for the node.
Description	Description of a user-defined node.
Maintained By	Select a node owner.

Step 7 Click **Confirm**.

----End

11.1.2.2 Partitioning a Disk

To keep collectors healthy for you to collect security data, there are some limitations and constraints.

- Only non-administrator users can be used for installing isap-agent.
- Make sure the **/opt/cloud** directory where you install isap-agent and use the collector has at least 100 GB of free disk space.

When you install the isap-agent in the **/opt** directory on an ECS, if the message shown in [Figure 11-7](#) is displayed, the space of the **/opt** directory is insufficient.

Figure 11-7 Insufficient disk space error

```



% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
             Dload  Upload    Total   Spent    Left   Speed
100 158k  100 158k  100  214  1819k  2459  --:--:--  --:--:--  --:--:-- 1821k
====Start check all params...====
====Check all params success!====
filesystem      Size Used Avail Use% Mounted on
devtmpfs        993M   0  993M   0% /dev
tmpfs           987M   0  987M   0% /dev/shm
tmpfs           987M  3.4M  984M   1% /run
tmpfs           987M   0  987M   0% /sys/fs/cgroup
dev/mapper/VolGroup-lv_root 8.8G  1.5G  6.9G  18% /
dev/ndal        976M  114M  796M  13% /boot
dev/mapper/VolGroup-lv_tmp  2.8G  6.1M  1.8G   1% /tmp
dev/mapper/VolGroup-lv_log  7.9G  214M  7.2G   3% /var/log
tmpfs           182M   0  182M   0% /run/udev/
Tip: The directory space of /opt is too small. Please mount a 100GB disk on the current machine and partition the disk. After p
itioning the disk, please copy command again and reinstall it. The disk partition command is as follows:
# /opt/cloud/isap-agent/action/agent_controller_linux.sh partition
root@

```

To ensure at least 100 GB space is available in the directory where the component controller isap-agent is installed, you may need to partition the disk.

The procedure is as follows:

Step 1 Apply for and attach a disk.

1. Log in to the management console.
2. Click  in the upper left corner and select the region and project.
3. In the upper left corner of the page, click  and choose **Compute > Elastic Cloud Server**. In the ECS list, click the name of the ECS where isap-agent is installed to go to the ECS details page.
4. Click the **Disks** tab. On the displayed page, click **Add Disk**.
5. On the displayed page, apply for a disk with **Disk Specifications** set to **100 GiB**.

For details, see *Elastic Volume Service User Guide*.

6. After the disk is successfully attached, you can view the attached disk on the **Disks** tab for the ECS.

After a data disk is attached to a server, you must log in to the server and initialize the disk before you can use the disk.

Step 2 Partition the disk.

1. Log in to the node where isap-agent is installed and run the following command to check the disk usage:

lsblk

Figure 11-8 Checking the disk size on a node

```

[root@host-192-168-0-100 cloud]# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda                                  252:0    0   40G  0 disk
├─vda1                               252:1    0    1G  0 part /boot
├─vda2                               252:2    0   19G  0 part
├─┌─VolGroup-lv_root                 253:0    0    9G  0 lvm  /
  │├─VolGroup-lv_tmp                 253:1    0    2G  0 lvm  /tmp
  │└─VolGroup-lv_log                 253:2    0    8G  0 lvm  /var/log
└─vdb                                252:16   0  100G  0 disk
[root@host-192-168-0-100 cloud]# _
    
```

2. Run the following command to partition the disk:

sh /opt/cloud/isap-agent/action/agent_controller_linux.sh partition

If the following information is displayed, the disk is partitioned successfully.

Figure 11-9 Disk partitions

```

vdb                                252:16   0  100G  0 disk
[root@host-192-168-0-100 cloud]# sh /opt/cloud/isap-agent/action/agent_controller_linux.sh partition
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        893M   0  893M   0% /dev
tmpfs           987M   0  987M   0% /dev/shm
tmpfs           987M  3.4M  984M   1% /run
tmpfs           987M   0  987M   0% /sys/fs/cgroup
/dev/mapper/VolGroup-lv_root 8.8G  1.5G  6.9G  18% /
/dev/vda1       976M  114M  796M  13% /boot
/dev/mapper/VolGroup-lv_tmp  2.0G  6.1M  1.8G   1% /tmp
/dev/mapper/VolGroup-lv_log  7.9G  214M  7.2G   3% /var/log
tmpfs           182M   0  182M   0% /run/user/0
/dev/vdb1       89G   57M   84G   1% /opt
/dev/vdb2       9.0G  37M   9.3G   1% /opt/cloud/logs
[root@host-192-168-0-100 cloud]#
    
```

Step 3 Reinstall the component controller isap-agent. For details, see [Managing Nodes](#).

----End


11.1.2.3 Managing Nodes

Scenarios

This topic describes how to perform operations such as [Viewing Nodes](#) and [Deregistering a Node](#).

Viewing Nodes

Step 1 Log in to the management console.

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

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

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

Step 5 On the **Nodes** tab, view the details about nodes.

If there are many nodes displayed, use filters to search for a specific one.


Table 11-5 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. If no heartbeat message is sent within 15 minutes, the node is marked as Disconnected .

Step 6 To view details about a node, click the node name.

----End

Deregistering a Node

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Components**.
- Step 5** On the **Nodes** tab, 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. If you no longer need the data collection function, you need to manually release those resources.


----End

11.1.2.4 Configuring a Component

Scenario

This topic describes how to configure a component.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Components**. Then, select the **Components** tab.
- Step 5** On the **Components** tab page, click **Edit Settings** 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 **Add Node** dialog box displayed, select a node and click **OK**.
- Step 7** Click **Save and Apply** in the lower right corner of the page.

Wait for a period of time. When the component status changes to **Applied completed**, the Logstash collector has been installed on the current node.

----End

11.1.2.5 Logstash Configuration Description

The data collector Logstash for tenant-side collection is customized by SecMaster. In different transmission scenarios, you can adjust parameter settings to obtain an optimal performance. This topic mainly covers how to tune log4j2.properties and jvm.options.

JVM Running Memory Configuration

Table 11-6 JVM running memory configuration

Parameter	Configuration Type	Default Value	Description
-Djava.awt.headless	boolean	true	Server side configuration. If it is set to "true", you can run an application in headless mode (without a keyboard or display). This parameter is used for data related services.
-XX:+UseConcMarkSweepGC	boolean	false	Concurrent Mark Sweep (CMS) garbage collector for the old generation.
-Xmn	String	1024M	The size of the heap for the young generation. If the collection pressure is high, adjust this value. The larger the heap size for the young generation, the smaller the number of garbage collection times, and the higher the collection efficiency. Xmn must be smaller than Xmx .
-Xmx	String	2048M	The total (maximum) heap size. A proper Xmx can prevent JVM from using excessive system resources to keep the application available and stable. If this parameter is set to a very small value, the collector will start garbage collection over and over again. This will affect collector performance.

Parameter	Configuration Type	Default Value	Description
-Djruby.jit.threshold	number	0	The specified method invocation count. When this threshold is reached, the JIT compiler of JRuby attempts to compile the local code of the method. You can adjust this value to obtain an optimal balance between startup time (compilation cost) and execution time performance
-XX:CMSInitiatingOccupancyFraction	number	75	CMS garbage collector. When the old generation usage reaches 75%, CMS garbage collection is triggered.
-Xms	String	20248M	The initial Java heap size. When JVM starts, it attempts to allocate the specified amount of memory to the heap. A proper initial heap size will free you from frequent heap size adjustments while the application is running.

log4j2 log configuration

Table 11-7 log4j2 log configuration

Parameter	Configuration Type	Default Value	Description
appender.json_console_slowlog.layout.compact	boolean	true	JSON slow query log output.
appender.json_console_slowlog.layout.type	String	JSONLayout	Layout type of JSON slow query logs. Retain the default value.
appender.json_console_slowlog.type	String	Console	Type of JSON slow query logs. Default value: Console , which means that logs are directly displayed on the console.
appender.json_console_slowlog.layout.eventEol	boolean	true	JSON slow query log output.



Parameter	Configuration Type	Default Value	Description
appender.json_console_slowlog.name	String	json_console_slowlog	Name of the JSON slow query log. Retain the default value.

11.1.2.6 Viewing Component Details

Scenarios

This topic describes how to view component details.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Components**. Then, select the **Components** tab.
- 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.
 - **View Settings**
Click **View Settings** in the upper right corner of the component to be viewed. The configuration details about the component are displayed on the right.
 - **Edit Settings**
 - a. Click **Edit Settings** in the upper right corner of the component to be viewed. The **Configuration Management** panel 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 displayed, select a node and click **OK**.
 - Editing node parameters: Click  next to the node name to expand the node configuration information and edit the node parameters.
 - Running parameters: Locate the row that contains the target node, click **Run Parameter** in the **Operation** column.
 - Removing a node: Locate the row that contains the target node and click **Removed** in the **Operation** column.

- Batch deletion: Select the nodes you want to remove and click **Batch Remove** in the upper left corner of the list.
 - Viewing historical versions: Click **Historical Version** in the lower right corner of the panel.
- c. Click **Save and Apply** in the lower right corner of the page.

----End

11.1.3 Collection Management

11.1.3.1 Adding and Editing a Connection

Scenario


This topic describes how to add and edit a 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.

Adding a Connection

Step 1 Log in to the management console.

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

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

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

Step 5 Add a data connection source.

1. On the **Connections** tab, click **Add**.
2. Configure the data connection source details.
 - **Connection Method:** Select **Source**.
 - **Connection Type:** Select the type of the data source.
 - Set other parameters based on the selected connection type. For details about the parameters, see [Source Connectors](#).
3. After the setting is complete, click **Confirm** in the lower right corner of the page.

Step 6 Add a data connection destination.

1. On the **Connections** tab, click **Add**.
2. Configure the data connection destination details.
 - **Connection Method:** Select **Destination**.
 - **Connection Type:** Select the type of the data destination.
 - Set other parameters based on the selected connection type. For details about the parameters, see [Destination Connectors](#).

- After the setting is complete, click **Confirm** in the lower right corner of the page.

----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 part of the page and choose **Security > SecMaster**.

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

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

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 displayed page, edit the data source type.

Step 7 Check the settings and click **Confirm** in the lower right corner of the page.

----End

11.1.3.2 Rules for Configuring Connectors

Source Connectors

SecMaster provides a wide range of source connectors for you to collect security data from your security products.

Table 11-8 Source connector types

Connector Type	In-use Logstash	Description
TCP	tcp	This collector is used to receive TCP logs. For details about the configuration rules, see Table 11-9 .
User file	file	This collector is used to receive logs in local files. For details about the configuration rules, see Table 11-10 .
UDP	udp	This collector is used to receive UDP logs. For details about the configuration rules, see Table 11-11 .

Connector Type	In-use Logstash	Description
OBS	obs	This collector is used to obtain log data from an OBS bucket. For details about the configuration rules, see Table 11-12 .
Kafka	kafka	This collector is used to obtain Kafka network log data. For details about the configuration rules, see Table 11-13 .
SecMaster	pipe	This collector is used to transfer SecMaster data to you. For details about the configuration rules, see Table 11-14 .
Elasticsearch	elasticsearch	This collector is used to read data from the Elasticsearch cluster. For details about the configuration rules, see Table 11-15 .

Table 11-9 TCP connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Port	port	number	1025	Yes	Port number of the collection node.
Codec	codec	string	plain	Yes	Encoding format <ul style="list-style-type: none"> • Plain: Read the original content. • Json: processes the content in JSON format.
Packet label	type	string	tcp	Yes	Used to label logs.

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
SSL_enable	ssl_enable	boolean	false	No	Whether to enable SSL verification.
SSL certificate	ssl_cert	file	null	No	Certificate.
SSL key	ssl_key	file	--	No	SSL key file.
SSL key passphrase	ssl_key_passphrase	string	--	No	SSL certificate key.

Table 11-10 File connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
File path	path	array	/opt/cloud/logstash/config/in.txt	Yes	Path to obtain files.
Start position	start_position	string	beginning	Yes	Read start position.
Decoding type	codec	string	json	Yes	Decoding type <ul style="list-style-type: none"> • Plain: Read the original content. • Json: Processes the content in JSON format.
Packet label	type	string	file	No	Packet label, which is used for subsequent processing.
Enable metric	enable_metric	boolean	true	No	Whether to enable metrics.

Table 11-11 UDP connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Port	port	number	1025	Yes	Port for the collection node.
Codec	codec	string	plain	Yes	Decoding type <ul style="list-style-type: none"> • Plain: Read the original content. • Json: Processes the content in JSON format.
Packet label	type	string	udp	No	Packet label, which is used for subsequent processing.
Queue size	queue_size	number	20000	No	Queue size.
Number of bytes in the receiving buffer	receive_buffer_bytes	number	20000	No	Number of bytes in the receiving buffer
Buffer size	buffer_size	number	10000	No	Buffer size
Worker thread	workers	number	1	No	Number of worker threads

Table 11-12 OBS connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
region	region	string	--	Yes	region
Bucket	bucket	string	demo-obs-sec-mrd-datas	Yes	OBS bucket name

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
endpoint	endpoint	string	--	Yes	Endpoint address. Note that https must be added.
AK	ak	string	--	No	AK
SK	sk	string	--	No	SK
Prefix	prefix	string	/test	No	Prefix of the folder for log reads
Cache folder	temporary_directory	string	/temp	No	Cache folder for log reads
Packet label	type	string	--	No	Packet label
Memory path	sincedb_path	string	/opt/cloud/logstash/pipeline/file_name	No	Log read position. This parameter is used to prevent full-text traversal caused by restart.

Table 11-13 Kafka connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Service address	bootstrap_servers	string	--	Yes	Service address
Topics	topics	array	logstash	Yes	Topics. Multiple topics can be consumed at the same time.
Consumer threads	consumer_threads	number	1	Yes	Consumer threads

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Auto offset reset	auto_offset_reset	string	latest	No	Offset reset <ul style="list-style-type: none"> • Earliest: Read the earliest message. • Latest: Read the latest messages.
SSL certificate	ssl_truststore_location	file	--	No	SSL certificate This parameter is mandatory when SSL is selected.
SSL private key	ssl_truststore_password	string	--	No	SSL private key This parameter is mandatory when SSL is selected.
Security protocol	security_protocol	string	SASL_SSL	No	Security protocol
SASL connection configuration	sasl_jaas_config	string	--	No	SASL connection configuration
Encrypted	is_pw_encrypted	string	false	No	Encrypted
SASL mechanism	sasl_mechanism	string	PLAIN	No	sasl_mechanism
Group ID	group_id	string	--	No	group_id
<p>Set sasl_jaas_config based on the Kafka specifications. Example:</p> <ul style="list-style-type: none"> • Plaintext connection configuration <code>org.apache.kafka.common.security.plain.PlainLoginModule required username='kafka user' password='kafka password';</code> • Ciphertext connection configuration <code>org.apache.kafka.common.security.scram.ScramLoginModule required username='kafka user' name' password='kafka password';</code> 					

Table 11-14 Pipe connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Type	type	string	Tenant	Yes	Type
Pipeline	pipeld	string	--	Yes	Pipeline ID
domain_name	domain_name	string	domain_name	Yes	Domain name of the user
User_name	user_name	string	user_name	Yes	Username of the user
Password	user_password	string	--	Yes	Username of the user
Subscription type	subscription_type	string	true	No	Subscription type <ul style="list-style-type: none"> • Shared: shared mode • Exclusive: exclusive mode • Failover: disaster recovery mode
Subscription Start	subscription_initial_position	string	true	No	Subscription Start

Table 11-15 Elasticsearch connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Hosts	hosts	array	--	Yes	Host IP address
Index	index	string	--	Yes	Index
Retrieval statement	query	string	--	Yes	Retrieval statement
User_name	user	string	--	Yes	User_name
Password	user_password	string	--	Yes	Password

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Queries	size	number	20	Yes	Queries
Scroll	scroll	string	5m	Yes	Volume
Docinfo	docinfo	boolean	true	Yes	Document
Is pw encrypted	is_pw_encrypted	boolean	true	Yes	Whether to enable encryption
Whether to enable SSL	ssl	boolean	true	No	Whether to enable SSL
Ssl	ca_file	file	--	No	Certificate file
Ssl_certificate_verification	ssl_certificate_verification	boolean	true	No	SSL certificate verification

Destination Connectors

SecMaster provides a wide range of destination connectors for you to collect security data from your security products.

Table 11-16 Destination connectors

Connector Type	In-use Logstash	Description
File	file	This collector is used to write data to local files on nodes. For details about the configuration rules, see Table 11-17 .
TCP	tcp	This collector is used to send TCP logs. For details about the configuration rules, see Table 11-18 .
UDP	udp	This collector is used to send UD logs. For details about the configuration rules, see Table 11-19 .
Kafka	kafka	This collector is used to write logs to Kafka message queues. For details about the configuration rules, see Table 11-20 .
OBS	obs	This collector is used to write logs to OBS buckets. For details about the configuration rules, see Table 11-21 .

Connector Type	In-use Logstash	Description
SecMaster pipeline	pipe	This collector is used to write logs to the SecMaster pipeline. For details about the configuration rules, see Table 11-22 .

Table 11-17 File connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Path	path	string	/opt/cloud/logstash/config/out.txt	Yes	File path on the output node
Create if deleted	create_if_deleted	boolean	true	Yes	If the file does not exist, create one.
Decoding type	codec	string	json_lines	Yes	Codec <ul style="list-style-type: none"> plain: Read the original content. Json_lines: Processes the content in JSON format.

Table 11-18 TCP connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Port	port	number	1025	Yes	Port

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Decoding type	codec	string	plain	Yes	Decoding type, which can be json_lines or Plain . <ul style="list-style-type: none"> • plain: Read the original content. • Json_lines: Processes the content in JSON format.
Hosts	host	string	192.168.0.66	Yes	Host address Note: The network between the host and the node is normal.
SSL certificate	ssl_cert	file	--	No	SSL certificates
Whether to enable SSL	ssl_enable	boolean	false	No	Whether to enable SSL authentication
SSL key	ssl_key	file	--	No	SSL certificate file
SSL key passphrase	ssl_key_passphrase	string	--	No	SSL certificate key

Table 11-19 UDP connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Hosts	host	string	--	Yes	Host IP address. Note: The network between the host and the node is normal.
Port	port	number	1025	Yes	Port
Decoding type	codec	string	json_lines	Yes	Decoding type, which can be Json_lines or Plain . <ul style="list-style-type: none"> plain: Read the original content. Json_lines: Processes the content in JSON format.
Retry count	retry_count	number	3	No	Time of retry attempts
Retry backoff (ms)	retry_backoff_ms	number	200	No	Retry backoff (ms)

Table 11-20 Kafka connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Service address	bootstrap_servers	string	--	Yes	Service address, for example, 192.168.21.21:9092,192.168.21.24:9999.

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Topics	topic_id	string	logstash	Yes	Topics
Decoding type	codec	string	plain	Yes	Decoding type, which can be Json or Plain .
Maximum length of the request	max_request_size	number	10485760	Yes	Maximum length of the request
SSL certificate	ssl_truststore_location	file	--	No	SSL certificates This parameter is mandatory when SSL is selected.
SSL private key	ssl_truststore_password	string	--	No	SSL private key This parameter is mandatory when SSL is selected.
Security protocol	security_protocol	string	PLAINTEXT	No	Security protocol
SASL connection configuration	sasl_jaas_config	string	--	No	SASL connection configuration
is_pw_encrypted	is_pw_encrypted	string	true	No	Whether to encrypt the value.
SASL mechanism	sasl_mechanism	string	PLAIN	No	sasl_mechanism

Rule	Logstash Settings	Type	Default Value	Mandator y	Description
<p>Set Sasl_jaas_config based on the Kafka specifications. The following is an example:</p> <ul style="list-style-type: none"> • Plaintext connection configuration <code>org.apache.kafka.common.security.plain.PlainLoginModule required username='kafka user' password='kafka password';</code> • Ciphertext connection configuration <code>org.apache.kafka.common.security.scram.ScramLoginModule required username='kafka user name' password='kafka password';</code> 					

Table 11-21 OBS connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandator y	Description
region	region	string	--	Yes	region
Bucket	bucket	string	demo-obs-sec-mrd-datas	Yes	Bucket name
endpoint	endpoint	string	--	Yes	endpoint
Cache folder	temporary_directory	string	/temp/logstash/	Yes	Cache path
Encoding type	codec	string	plain	No	Encoding format: plain or JSON
AK	ak	string	--	No	AK
SK	sk	string	--	No	SK
Prefix	prefix	string	test	No	Path prefix.
Encoding format	encoding	string	gzip	No	Encoding format: gzip or pure file
Memory path	sincedb_path	string	/opt/cloud/logstash/pipeline/file_name	No	Log read position. This parameter is used to prevent full-text traversal caused by restart.

Table 11-22 Pipe connector configuration rules

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Type	type	string	Tenant	Yes	Type
Pipeline	pipeld	string	--	Yes	Pipeline
AK	ak	string	--	Yes	AK This parameter is mandatory when the platform type is selected.
SK	sk	string	--	Yes	SK This parameter is mandatory when the platform type is selected.
domain_name	domain_name	string	domain_name	Yes	Domain name of the user This parameter is mandatory when the tenant type is selected.
User_name	user_name	string	user_name	Yes	Username of the user This parameter is mandatory when the tenant type is selected.
Password	user_password	string	--	Yes	Password of the user This parameter is mandatory when the tenant type is selected.

Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Compression type	compression_type	string	NONE	No	Packet compression type
Block if the queue is full	block_if_queue_full	boolean	true	No	Whether to block the access if the queue is full.
Enable batch processing	enable_batching	boolean	true	No	Whether to enable batch processing.

11.1.3.3 Managing Connections

Scenarios

This section describes how to perform the following operations: [Deleting a Data Connection](#) and [Deleting a Data Connection](#).

Viewing Connections


- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Collections**.
- Step 5** On the **Connections** tab, view connection details.


Table 11-23 Connection parameters

Parameter	Description
Connection Name	Connection name
Connection Type	Connection type
Connection Info	Information about the connection
Channel	Number of channels that are used by the connection
Description	Description of the connection
Operation	Operations such as editing or deleting connections

----End

Deleting a Data Connection

Step 1 Log in to the management console.

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

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

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

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

11.1.3.4 Creating and Editing a Parser

Scenario

By default, SecMaster has a built-in quick access parser. You can select a parser as required.


Table 11-24 Parser scenario description

Type	Scenario
Quick access	The source data can be directly transmitted without being processed.
Template	When you need to clear data sources or process fields, you can select a template based on the application scenario and create a parser.
Custom	You can create custom parsers and configure parsing rules to meet your needs, such as clearing data sources, processing fields, and more.

This topic describes how to create and edit a parser.

Creating a Parser

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Parsers** tab.

Step 5 [Customize a parser](#) or [create a parser from a template](#).

- **Customizing a parser**
 - a. On the **Parsers** tab page, click **Add**.
 - b. On the **Parsers** tab page, set parameters.

Table 11-25 Parameters for adding a parser

Parameter		Description
Basic Information	Parser Name	Set the parser name.
	Description	Enter the parser description.
Rule list		<p>Set the parsing rule of the parser. Perform the following steps:</p> <ol style="list-style-type: none"> 1. Click Add and select a rule type. <ul style="list-style-type: none"> ○ Parsing rule: Select the parsing rule of the parser. For details about the parameters, see Rules for Configuring Parsers. ○ 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. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.
- **Creating a parser from a template**
 - a. On the **Parsers** tab page, click the **Templates** tab.
 - b. On the displayed page, locate the row that contains the target template, click **Created by Template** in the **Operation** column.
 - c. On the **Parsers** tab page, set parameters.

Table 11-26 Parameters for adding a parser

Parameter		Description
Basic Information	Parser 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.


Parameter	Description
Rule list	<p>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 rule: Select the parsing rule of the parser. For details about the parameters, see Rules for Configuring Parsers. ▪ Conditional control: Select the conditions for the parser. You can select If, Else, or Else if.

- d. After the setting is complete, click **OK** in the lower right corner of the page to confirm the setting.

----End

Editing a Parser

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Parsers** tab.

Step 5 On the **Parsers** tab, 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 11-27 Editing a parser

Parameter		Description
Basic Information	Parser Name	Set the parser name.
	Description	Enter the parser description.

Parameter	Description
Rule list	<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. For details about the parameters, see Rules for Configuring Parsers. ● Conditional control: Select the conditional 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

11.1.3.5 Rules for Configuring Parsers

The tenant-side data collection uses custom Logstash collectors for data transmission. Parsers mainly work as codeless filters in Logstash. Currently, the following types of Logstash filter plugins are supported.

Table 11-28 Supported types

Parser	Plug-in in Logstash	Description
Key-Value filter	kv	Parses key-value pairs. For details about parsing rules, see Table 11-29 .
Mutate filter	mutate	Performs general mutations on fields. For details about parsing rules, see Table 11-30 .
Grok filter	grok	Parses regular expressions. For details about parsing rules, see Table 11-31 .
Date filter	date	Parses the date. For details about parsing rules, see Table 11-32 .
Drop filter	drop	Deletes packets. There is no specific rule. If you use this parser, logs received will be deleted.
Prune filter	prune	Parses blacklists and whitelists. For details about parsing rules, see Table 11-33 .
CSV filter	csv	Parses the CSV data. For details about parsing rules, see Table 11-34 .

Parser	Plug-in in Logstash	Description
Function filter	ruby	Executes ruby code. For details about parsing rules, see Table 11-35 .
JSON filter	json	Converts the JSON data. For details about parsing rules, see Table 11-36 .
Split filter	split	Splits data. For details about parsing rules, see Table 11-37 .
Clone filter	clone	Duplicates data. For details about parsing rules, see Table 11-38 .
UUID filter	uuid	Parses UUIDs. For details about parsing rules, see Table 11-39 .

Table 11-29 Kv filter

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Source	source	string	source	Yes	Defines the fields to be translated.
Target	target	string	message	No	Defines the target fields.
Field_split	field_split	string	,	No	Splits fields.
Value_split	value_split	string	=	No	Splits fields.
Trim_key	trim_key	string	--	No	Removes spaces from the key.
Trim_value	trim_value	string	--	No	Removes spaces from the value.
Allow_duplicate_values	allow_duplicate_values	boolean	true	No	Allows duplicate values.
Default_keys	default_keys	array	--	No	Adds keys.
Exclude_keys	exclude_keys	array	--	No	Excludes certain keys.
Include_keys	include_keys	array	--	No	Includes certain keys.

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Prefix	prefix	string	--	No	Performs prefix matches.
Recursive	recursive	boolean	true	No	Performs Recursive parsing.
Transform_key	transform_key	string	--	No	Transforms keys.
Add_field	add_field	hash	--	No	Adds fields.
add_tag	add_tag	array	--	No	Adds tags.
Remove_field	remove_field	array	--	No	Removes fields.
Remove_tag	remove_tag	array	--	No	Removes tags.
Id	id	string	--	No	ID.
Whitespace	whitespace	string	strict/lenient	No	Allows whitespace characters.
Remove_char_key	remove_char_key	string	<>[](),	No	Removes characters from the key.

Table 11-30 Mutate filter

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Convert	convert	hash	--	No	Converts a field's value into a different type.
Join	join	hash	--	No	Joins arrays.
Lowercase	lowercase	array	--	No	Converts characters into its lowercase equivalent.

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Coerce	coerce	hash	--	No	Sets the default value of a field.
Rename	rename	hash	--	No	Renames fields.
Replace	replace	hash	--	No	Replaces the value of a field with a new value.
Split	split	hash	--	No	Split a field to an array.
Strip	strip	array	--	No	Strips spaces from fields.
Update	update	hash	--	No	Updates fields.
Uppercase	uppercase	array	--	No	Converts characters into its uppercase equivalent.
Add_field	add_field	hash	--	No	Adds fields.
Add_tag	add_tag	array	--	No	Adds tags.
Remove_field	remove_field	array	--	No	Removes fields.
Remove_tag	remove_tag	array	--	No	Removes tags.
ID	id	string	--	No	Id
Copy	copy	hash	--	No	Copies fields.
Gsub	gsub	array	--	No	Replaces the gsub value.

Table 11-31 Grok filter

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
match	match	hash	--	Yes	Performs regex matches.
Break_on_match	break_on_match	boolean	true	No	Breaks on the first match.
Overwrite	overwrite	array	message	No	Overwrites fields.
Add_field	add_field	hash	--	No	Adds fields.
Add_tag	add_tag	array	--	No	Adds tags.
Remove_field	remove_field	array	--	No	Removes fields.
Remove_tag	remove_tag	array	--	No	Removes tags.
Id	id	string	--	No	Id

Table 11-32 Date filter

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Match	match	array	--	Yes	Performs regex match.
Target	target	string	timestamp	Yes	Target fields.
Add_field	add_field	hash	--	No	Adds fields.
Add_tag	add_tag	array	--	No	Adds tags.
Remove_field	remove_field	array	--	No	Removes fields.
Remove_tag	remove_tag	array	--	No	Removes tags.
Id	id	string	test	No	Id
Locale	locale	string	--	No	Locale
Timezone	Specifies the time zone.	string	+8:00	No	Specifies the time zone.

Table 11-33 Prune filter

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Blacklist_names	blacklist_names	array	--	No	Excludes fields whose names match specified regular expressions.
Blacklist_values	blacklist_values	array	--	No	Excludes specified fields if their values match one of the supplied regular expressions.
Whitelist_names	whitelist_names	array	--	No	Includes specified fields only if their names match specified regular expressions.
Whitelist_values	whitelist_values	array	--	No	Includes specified fields only if their values match one of the supplied regular expressions.

Table 11-34 CSV filter

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Source	source	string	message	No	Defines the fields to be parsed.
Columns	columns	array	--	No	Defines a list of column names.

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Separator	separator	string	,	No	Defines the column separator value.
Skip_empty_columns	skip_empty_columns	boolean	true	No	Defines whether empty columns can be skipped.

Table 11-35 Function filter

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Filter_length	filter_length	number	10	No	Controls the field length.
Set_time	set_time	ruby_time	123	No	Sets a time.

Table 11-36 JSON filter

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Source	source	string	message	Yes	Defines source fields.
Skip_on_invalid_json	skip_on_invalid_json	boolean	true	No	Skips invalid json fields.
Add_field	add_field	hash	null	No	Adds fields.
Add_tag	add_tag	array	null	No	Adds tags.
Remove_field	remove_field	array	null	No	Removes fields.
Remove_tag	remove_tag	array	null	No	Removes tags.
Target	target	string	message	No	Defines target fields.

Table 11-37 Split filter

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Field	field	string	message	Yes	Defines fields to be splitted.

Table 11-38 Clone filter

Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Clone	clones	array	--	Yes	Defines the list of fields to be cloned.

Table 11-39 UUID filter


Parsing Rule	Logstash Settings	Type	Default Value	Mandatory	Description
Target	target	string	uuid	Yes	Target fields.
Overwrite	overwrite	boolean	true	Yes	Defines whether to overwrite.

11.1.3.6 Managing Parsers

Scenarios

This topic describes how to perform the following operations: [Viewing Parsers](#), [Importing a Parser](#), [Exporting a Parser](#), and [Deleting a Parser](#).

Viewing Parsers

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Parsers** tab.

Step 5 On the **Parsers** page, view the detailed information about parsers.

Table 11-40 Parsers parameters

Parameter	Description
Name	Name of the parser.
Channel	Number of channels that are used by the parser
Description	Description of the parser.
Operation	Operations such as editing or deleting the parser

Step 6 On the **Parsers** page, click the **Templates** tab.

Step 7 On the **Templates** tab displayed, view the parser templates you can use.

Table 11-41 Parser template parameters

Parameter	Description
Name	Name of a parser template
Description	Description of the parser template
Operation	Creating a parser from a template.


----End

Importing a Parser

NOTE

- Only .json files no larger than 1 MB can be imported.
- A maximum of five parser files can be imported at a time, and each parser file can contain a maximum of 100 parsers.

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Parsers** tab.

Step 5 On the **Parsers** tab, click **Import** in the upper left corner above the parser list.

Step 6 In the displayed **Import** dialog box, click **Select File** and select the JSON file you want to import.

CAUTION

- Only .json files no larger than 1 MB can be imported.
 - A maximum of five parser files can be imported at a time, and each parser file can contain a maximum of 100 parsers.
-


Step 7 Click **OK**.

You can view imported parsers in the parser list.

----End

Exporting a Parser

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Parsers** tab.


Step 5 On the **Parsers** page, select the parsers you want to export and click **Export** above the list.

The system automatically downloads the parser file in .json format to your local PC.

----End

Deleting a Parser

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Parsers** tab.

Step 5 On the **Parsers** tab, 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

11.1.3.7 Adding and Editing a Collection Channel


Scenario

This topic describes how to add and edit a collection channel.

Adding a Channel Group

Before adding a collection channel, you need to add a connection group.



Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Collection Channels** tab.

Step 5 Add a channel group.


1. On the **Collection Channels** tab, click  on the right of **Groups**.
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.

----End

Adding a Collection Channel

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Collection Channels** tab.

Step 5 On the right of the group list, click **Add**.

Step 6 On the displayed page, in the **Basic Configuration** phase, configure basic information.

Table 11-42 Basic configuration parameters

Parameter		Description
Basic Information	Title	User-defined collection channel name.
	Channel grouping	Select the group to which the collection channel belongs.
	(Optional) Description	(Optional) Enter the description of the collection channel.

Parameter		Description
Configure Source	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 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 **Configure Parser** page, select a parser. You can check its details.

If no parser is available or you want to create a parser, click **Create** and create one. For details, see [Creating and Editing a Parser](#).

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 **Create**. In the **Add Node** dialog box displayed, select a node and click **OK**.

- Running parameters: You can configure running parameters for added nodes by taking 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 select a key and value.

If you need to optimize the running parameters of a collection channel, SecMaster provides optimization parameters **pipeline.batch.size**, **pipeline.workers**, and **pipeline.batch.delay** for your choice. If no optimizations are required, delete related configurations.

Table 11-43 Parameter configuration description

Parameter	Type	Description
pipeline.batch.size	int	This parameter specifies the number of events that can be collected by each worker thread each time. A larger value indicates a higher efficiency. However, the memory overhead also increases. You can increase the heap space in jvm.options .

Parameter	Type	Description
pipeline.workers	int	This parameter specifies the number of worker threads in the pipeline. The default value is the number of CPU cores.
pipeline.batch.delay	int	This parameter specifies the delay to submit the current pipeline. You can use this parameter to increase message submission times and system consumption efficiency.

- 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 **Preview Channel Details** page, confirm the configuration and click **Save and Execute**.

If the collection channel healthy status is **Normal**, all collection channels are successfully delivered. The following table describes the statuses of collection channels.


Table 11-44 Health status of a collection channel

Monitoring Status	Description
Healthy	The collection channel is successfully delivered.
Abnormal	Some collection channels are successfully delivered, and some are abnormal.
Faulty	The collection channel has not been delivered. This status changes according to the heartbeat status, and there is a delay. Generally, the monitoring status is reported every 30 seconds.

----End

Editing a collection channel

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Collection Channels** tab.

- 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.

Table 11-45 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.
	(Optional) Description	(Optional) Enter the description of the collection channel.
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 [Creating and Editing a Parser](#).
- 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 **OK**.
- **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 select a key and value.
 - 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 **Preview Channel Details** page, confirm the configuration and click **Save and Execute**.

----End

11.1.3.8 Managing Collection Channels

Scenarios

This topic describes how to perform the following operations: [Viewing Collection Channels](#), [Deleting a Collection Channel](#), and [Enabling, Disabling, and Restarting a Collection Channel](#).

Viewing Collection Channels



- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Collection Channels** tab.
- Step 5** On the **Collection Channels** page, view the detailed information about collection channels.

Table 11-46 Collection channel parameters

Parameter	Description
Groups	List of collection channel groups and group names.
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.
Receiving Rate	Data receiving rate of the collection channel.
Sending Rate	Data sending rate of the collection channel.
Configuration Status	Configuration status of the collection channel.
Channel Instance	Number of collection channels.
Delivery Status	Status of a collection channel.
Operation	Operations such as editing and disabling a collection channel.

----End

Deleting a Collection Channel

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Collection Channels** tab.
- 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, and Restarting a Collection Channel

- Step 1** Log in to the management console.
- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Collection Channels** tab.
- 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


11.1.3.9 Viewing Collection Nodes

Scenario

This topic describes how to view collection nodes details.

Procedure

- Step 1** Log in to the management console.

- Step 2** Click  in the upper part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Collection Nodes** tab.
- Step 5** On the **Collection Nodes** page, view the detailed information about collection nodes.

If there are many nodes displayed, use filters to search for a specific one.

To view details about a node, click its name to go to its details page.

Table 11-47 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. If no heartbeat message is sent within 15 minutes, the node is marked as Disconnected .

----End

11.1.4 Upgrading the Component Controller

Scenarios


This topic describes how to upgrade the component controller from salt-minion to isap-agent for tenant-side data collection. salt-minion was used as component controller in earlier tenant-side data collection.

 **NOTE**

The upgrade does not affect the data plane.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Deregister a node.

1. In the navigation pane on the left, choose **Settings > Components**. On the displayed **Nodes** tab, locate the row that contains the target node and click **Deregister** in the **Operation** column.

2. In the displayed dialog box, click **OK**.

The node is deregistered successfully, and its **Health Status** changes to **Disconnected**.

Step 5 Copy the script.

1. On the **Nodes** page, click **Create**.

2. On the **Create Node** page, click **Next**. On the **Verify installed Script** page, copy the script.

Step 6 Install the component controller.

1. Use a remote management tool, such as Xftp, SecureFX, WinSCP, PuTTY, or Xshell, to log in to the disconnected ECS node.

2. Run the command copied in [Step 5.2](#) as user **root** to install the Agent on the ECS.

Figure 11-10 Installing the agent

```

1/54214ac93c18dc9bd418161e388381/workspaces/7b9fd73c6b-4cdf-b2bf-d1f79ad28cf2/collector/files/isap-agent.tar.gz && tar -xvz
f_zopt/cloud/isap-agent.tar.gz -C zopt/cloud && sh zopt/cloud/isap-agent.sh 54214ac93c18dc9bd418161e388381 7b9fd73c6b-4cdf-
b2bf-d1f79ad28cf2 https://secmaster-ga.cn-north-7.myhuaweicloud.com https://iam.cn-north-7.myhuaweicloud.com/v3/auth/tokens
% Total % Received % Xferd Average Speed Time Time Current
 Dload Upload Total Spent Left Speed
100 4070k 0 4070k 0 0 48.0M 0 --:--:-- --:--:-- 41.0M
./csb-isap-agent-service_1.0_20240725142527_all.tar.gz
./isap-agent.sh
csb-isap-agent-service_1.0_20240725142527_all/
csb-isap-agent-service_1.0_20240725142527_all/csb-isap-agent-service_1.0_20240725142527_x86_64.tar.gz
csb-isap-agent-service_1.0_20240725142527_all/csb-isap-agent-service_1.0_20240725142527_arch64.tar.gz
csb-isap-agent-service_1.0_20240725142527_x86_64/
csb-isap-agent-service_1.0_20240725142527_x86_64/var/
csb-isap-agent-service_1.0_20240725142527_x86_64/bin/
csb-isap-agent-service_1.0_20240725142527_x86_64/bin/csb-isap-agent-service
csb-isap-agent-service_1.0_20240725142527_x86_64/manifest.yml
csb-isap-agent-service_1.0_20240725142527_x86_64/action/
csb-isap-agent-service_1.0_20240725142527_x86_64/action/overtimeIninstall.sh
csb-isap-agent-service_1.0_20240725142527_x86_64/action/agent_controller_linux.sh
csb-isap-agent-service_1.0_20240725142527_x86_64/repov/
csb-isap-agent-service_1.0_20240725142527_x86_64/conf/
csb-isap-agent-service_1.0_20240725142527_x86_64/conf/banner.txt
csb-isap-agent-service_1.0_20240725142527_x86_64/conf/config.properties
csb-isap-agent-service_1.0_20240725142527_x86_64/conf/component.properties
csb-isap-agent-service_1.0_20240725142527_x86_64/conf/isap-agent.service
Please enter your IAM Account doMainName: s-*****02
Please enter your IAM Account userName:
Please enter your IAM Account Password: *****
% Total % Received % Xferd Average Speed Time Time Current
 Dload Upload Total Spent Left Speed
100 168k 100 168k 100 217 154k 199 0:00:01 0:00:01 --:--:-- 155k
[====Start check all params.====]
[====Check all params success!====]
service user has exist
chown: invalid group: 'service:service'
chown: invalid group: 'service:service'
chown: invalid group: 'service:service'
311200
chown: invalid group: 'service:service'
start to install isap-agent, please wait ....
start to install isap-agent, please wait ....
root 811200 811115 0 11:43 tty1 00:00:00 zopt/cloud/isap-agent/bin/csb-isap-agent-service
root 811300 811115 0 11:43 tty1 00:00:00 grep csb-isap-agent-service
311200
=====
install isap-agent successfully
=====
[root@localhost conf]#

```

3. Enter the account username and password as prompted.

4. If information similar to the following is displayed, the agent is successfully installed:

```
install isap-agent successfully
```

5. Go to the SecMaster console and check the node status on the **Nodes** page under **Settings**.

Step 7 Delete the old management channel.

1. Choose **Settings > Components > Nodes** and click **Create**. On the **Create Node** pane displayed, click **Delete** in the **Operation** column in the row of each the management.
2. In the displayed dialog box, click **OK**.

----End

11.2 Data Integration

11.2.1 Log Access Supported by SecMaster

SecMaster can integrate logs of multiple cloud products. You can search for and analyze all collected logs in SecMaster.

Table 11-48 Log access supported by SecMaster

Category	Service	Service Type	Log	Log Description
Host security	Host Security Service (HSS)	Tenant-side cloud service	hss-alarm	HSS alarms
			hss-vul	HSS vulnerability scan results
			hss-log	HSS logs
Application security	Web Application Firewall (WAF)	Tenant-side cloud service	waf-attack	WAF attack logs
			waf-access	WAF access logs
	Cloud Trace Service (CTS)	Tenant-side cloud service	cts-audit	CTS logs
O&M security	Cloud Bastion Host (CBH)	Tenant-side cloud service	cbh-audit	Bastion host audit logs

11.2.2 Enabling Log Access

Scenario

SecMaster can access logs of multiple cloud products with your authorization. After you authorize the access, you can manage logs centrally and search and analyze all collected logs.


This topic describes how to access logs and view where logs are stored.

Limitations and Constraints

It takes about 10 minutes for the log access settings to take effect.


Allowing SecMaster to Access Service Logs


Step 1 Log in to the management console.

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

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

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


Step 5 Locate the cloud service from which you want to collect logs, click  in the **Logs** column to enable log access.

To access logs of cloud services supported in the current region, click  on the left of **Access Service Logs**.

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**.

Locate the row containing the target security products. In the **Automatically converts alarms** column of that row, click  to enable the function. After that, SecMaster will automatically convert cloud service logs into alerts when the logs meet certain alert rules. Those alerts will be displayed 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**. In the displayed dialog box, click **OK**.


NOTE

It takes about 10 minutes for the log access settings to take effect. 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 part of the page and choose **Security > SecMaster**.



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

Step 4 In the navigation pane 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
 - a. In the **Log** column of the target cloud services, click  to disable the access to cloud service logs.
 - b. Click **Save**.
- Editing the Data Access Lifecycle
 - a. In the **Lifecycle** column of the target cloud services, enter the data storage period.
 - b. Click **Save**.
- Canceling Automatic Converting Logs to Alarms
 - a. In the **Automatically converts alarms** column of the target cloud products, click  to disable the alarms.
 - b. Click **Save**.

11.3 Customizing Directories

Scenario

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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation tree on the left, choose **Settings > Directory Customization**.

Step 5 In the directory list, view the directory details.


Table 11-49 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 part of the page and choose **Security > SecMaster**.

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

Step 4 In the navigation tree on the left, choose **Settings > Directory Customization**.

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

12 FAQs

12.1 Product Consulting

12.1.1 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 little to the Internet (risks such as open ports and weak passwords can be exploited by attackers), it is less likely that they will be attacked. So there will be no or little security data in SecMaster.

12.1.2 Where Does SecMaster Obtain Its Data From?

SecMaster utilizes threat data collected from cloud-based threats and cloud services. Through big data mining and machine learning, it analyzes and presents threat trends while providing protection suggestions.

- SecMaster collects data from network traffic and security device logs to present the security status of assets and generate corresponding threat alerts using AI analysis.
- 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.

12.1.3 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 12-1 describes the differences between SecMaster and other security protection services.

Table 12-1 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.
Host Security Service (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 checks website service traffic in multiple dimensions. It can defend against common attacks and block threats to website. 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.

12.1.4 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 12-2 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.
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.

12.1.5 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 part of the page and choose **Security > SecMaster**.
- Step 3** In the navigation pane on the left, choose **Workspaces > Management**. In the workspace list, click the name of the target workspace.
- Step 4** In the navigation pane 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 > Alerts**. On the displayed page, handle the alert.
- Step 7** After handling unsafe settings, vulnerabilities, or alerts, go back to the **Security Situation > Situation Overview** page and click **Check Again**. After the check, the security score will be updated.

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

12.1.6 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 part of the page and choose **Security > SecMaster**.

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

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

Step 5 On the **Alert** tab, select **Brute-force attacks** and refresh the alert list.

Step 6 Delete the non-threat alerts.

----End

12.1.7 Issues About Data Synchronization and Data Consistency

Why Is the Data in SecMaster Inconsistent with That in WAF or HSS?

SecMaster aggregates all historical alert data reported by WAF and HSS, but WAF and HSS display real-time alert data. So data in SecMaster is inconsistent with that in WAF and HSS.

So you can go to the corresponding service (WAF or HSS) to view and handle latest alerts.

Why Is Zero Displayed for Total Assets on the Security Overview Page?

Symptom

A workspace was added and asset information was synchronized to and displayed on the **Resource Manager** page in the workspace, but the total number of assets on the **Security Overview** page is still 0.

Cause

SecMaster synchronizes asset details **every hour on the hour** after you create a workspace and synchronize asset information to the **Resource Manager** page.

Solution

Check the asset quantity after the very beginning of the next hour.

12.2 About Data Collection Faults

12.2.1 Component Controller Installation Failure

A component controller (isap-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.

For details about common commands used during troubleshooting, see [Common Commands for the Component Controller](#).

Possible Causes

The possible causes are as follows:

- The network between the ECS where you want to install component controller isap-agent and the OBS bucket storing the agent is disconnected.
- The disk space of the ECS server is insufficient.
- Failed to verify the workspace ID.
- The component controller isap-agent has been installed. The system attempts to install it again.

Locating the Cause and Fixing the Failure

- **The network between the ECS where you want to install component controller isap-agent and the OBS bucket storing the agent is disconnected.**

Figure 12-1 Disconnected network between the server and OBS

```
[root@host-192.168.0.29 ~]# wget http://cbs-isap-logstash.obs.cn-north-1.com/isap-wait-obs-agent-controller-euler.sh && chmod +x agent_controller_euler.sh && ./agent_controller_euler.sh install c18-4492-2c-5b6d019 c145a00f6c [*192.168.0.29*:*192.168.0.1*]
[*192.168.0.13:09:20:28*:*https://cbs-isap-logstash.obs.cn-north-1.com/isap-wait-obs-agent-controller-euler.sh
Resolving cbs-isap-logstash.obs.cn-north-1.com (cbs-isap-logstash.obs.cn-north-1.com)... failed: Name or service not known.
wget: unable to resolve host address 'cbs-isap-logstash.obs.cn-north-1.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.
 - i. Log in to the OBS management console.
 - ii. 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 12-2 Insufficient disk space



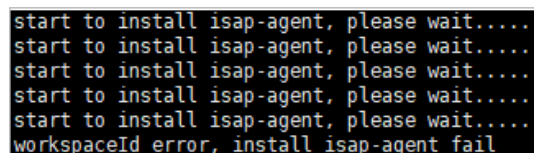
Solution

Clear the disk to reserve sufficient space.

- **Failed to verify workspace ID.**
 - **Symptoms**

If the information shown in the following figure is displayed, the Workspace ID verification fails.

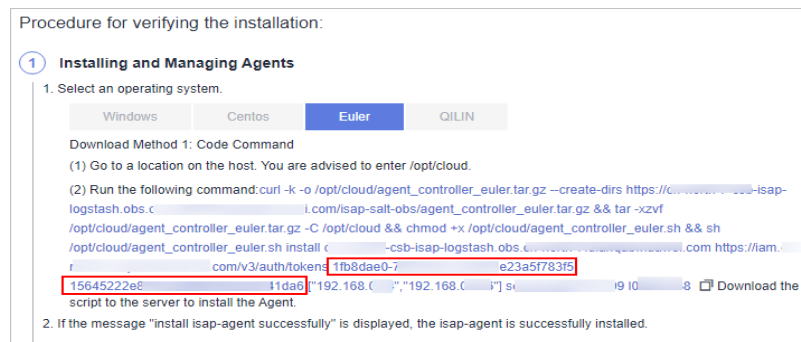
Figure 12-3 Workspace ID verification failure



Solution

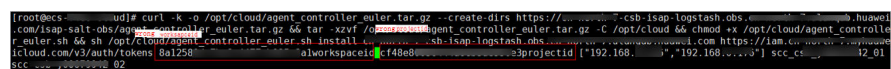
- **Solution**
 - i. Log in to the SecMaster management console.
 - ii. In the navigation pane on the left, choose **Workspaces**. In the workspace list, click the name of the target workspace.
 - iii. In the navigation pane on the left, choose **Settings > Components**. On the displayed page, click the target node.
 - iv. Check workspace ID and project ID in the command output.

Figure 12-4 Parameters on the console



- v. Check whether the workspace ID and project ID in the command are the same as those in the file in [iv](#).

Figure 12-5 Parameter information in the command

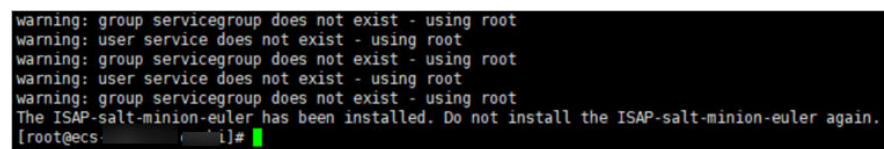


- vi. Use the correct workspace ID and project ID to run the command again.
- **The component controller isap-agent has been installed. The system attempts to install it again.**

- **Symptoms**

If the information shown in the following figure is displayed, the Agent has been installed.

Figure 12-6 Agent installed already



- **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 on the left, choose **Workspaces**. In the workspace list, click the name of the target workspace.
 - 3) In the navigation pane on the left, choose **Settings > Components**. On the displayed **Nodes** tab, locate the row that contains the target node and click **Deregister** in the **Operation** column.
 - 4) In the displayed dialog box, click **OK**.
- ii. (Optional) Method 2: Run a script command to uninstall component controller isap-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 component controller.

- 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 12-7 Script file

```
[root@ecs-...]# 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 12-8 Checking isap-agent details

```
[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.

12.2.2 Collection Node or Collection Channel Faults

Symptom

The component controller isap-agent periodically reports the collection node status and collection channel health status. Despite a delay of about one minute, the **Health Status** of a collection node or collection channel was still displayed as **Faulty** 3 minutes after the collection channel is delivered, and the CPU usage or memory usage of the server is about to reached 100%.

Figure 12-9 Collection node fault

Node NameID	Health Status	Region	IP Address	CPU Usage	Memory Usage	Disk Usage	Network Speed	Channel Instance	Tag	Heartbeat Disconnection Flag
444-...	Faulty		192.168.0.1	97.487142%	75.00% 308/408	13.00% 1308/19008	10.00MB/s W/ 0MB/s	3		Online 19902(7h38m10Z)
444-...	Normal		192.168.0.2	2.5%	55.00% 208/408	6.50% 1308/20008	10.00MB/s W/ 0MB/s	4		Online 19902(7h38m10Z)

Figure 12-10 Collection channel fault

Groups	Name	Connection Information	Created By	Health Status	Receiving Rate	Sending Rate	Configuration	Channel Instance	Delivery Status	Operation
All	emr_gar...	(Source Name) emr_gar...		Faulty	0 Slice/Second	0 Slice/Second	Synchronized	2	Running (-)	Enable Stop Restart More
	syslog...	(Source Name) syslog...		Normal	0 Slice/Second	0 Slice/Second	Synchronized	2	Running (-)	Enable Stop Restart More

Possible Causes

The configured connector or parser has syntax or semantic errors. As a result, the collector cannot run properly and restarts over and over again. The CPU and memory are exhausted.

Fault Location

1. Remotely log in to the ECS where the collection node resides.
 - 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 component controller on the server as user **root**.
2. Run the following command to check the OS running status:

top

If the following information is displayed, the Java process in the ECS uses a large number of CPU resources.

Figure 12-11 Status

```
top - 19:21:09 up 8 days, 29 min, 2 users, load average: 1.04, 0.29, 0.13
Tasks: 84 total, 1 running, 83 sleeping, 0 stopped, 0 zombie
%Cpu(s): 95.8 us, 3.7 sy, 0.0 ni, 0.5 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 3879596 total, 532820 free, 1234536 used, 2112240 buff/cache
KiB Swap: 0 total, 0 free, 0 used, 2295348 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM     TIME+ COMMAND
 29442 root        20   0 4731800 1.0g 15528 S 190.3 27.9   0:44.63 java
 29245 root        20   0 353640 30420 16508 S  0.7  0.8   0:00.23 dockerd
 29425 root        20   0 11780 5464 2740 S  0.7  0.1   0:00.02 containerd-shim
    9 root         0   0 0 0 0 S  0.3  0.0   1:41.10 rcu_sched
23490 root        20   0 830056 9704 4360 S  0.3  0.3   0:02.47 csb-isap-agent-
```

3. Run the following command to view the collector run logs:

docker logs isap-logstash -f

According to the logs, the filter (parser) configuration of the current collection channel is incorrect, as shown in the following figure.

Figure 12-12 Collector run log

```
-75 -XX:-UseConcMarkSweepGC, -Xmn1024M, -Djava.awt.headless=true, -Diruby.jit.threshold=0]
19:29:52.441 [main] INFO logstash.settings - Creating directory {setting=>"path.queue", :path=>"/opt/cloud/logstash/data/queue"}
19:29:52.452 [main] INFO logstash.settings - Creating directory {setting=>"path.dead_letter_queue", :path=>"/opt/cloud/logstash/data/dead_letter_queue"}
19:29:53.071 [LogStash::Runner] INFO Logstash.agent - No persistent UUID file found. Generating new UUID {uuid=>"496252c6-e46b-4e48-82b3-1b3d27664db2", :path=>"/opt/cloud/logstash/data/uuid"}
19:29:54.574 [Api Webserver] INFO Logstash.agent - Successfully started Logstash API endpoint {:port=>9600, :ssl_enabled=>false}
19:29:56.063 [Converge PipelineAction::Create:2aac87a8-c8b5-4cc8-8bbb-f74fe1314ca1] ERROR Logstash.agent - Failed to execute action {action=>LogStash::PipelineAction::Create/pipeline_id:2aac87a8-c8b5-4cc8-8bbb-f74fe1314ca1, :exception=>LogStash::ConfigurationError, :message=>"Expected one of [\\t\\r\\n], \\s\\*, \\{\\} at line 15, column 6 (byte 1463) after filter {unless " , :backtrace=>["/opt/cloud/logstash/logstash-core/lib/logstash/compiler.rb:32:in `compile_imperative'"/opt/cloud/logstash/execution/AbstractPipelineExt.java:189:in `initialize'", "org/logstash/execution/JavaBasePipelineExt.java:72:in `initialize'", "/opt/cloud/logstash/logstash-core/lib/logstash/java_pipeline.rb:48:in `initialize'", "/opt/cloud/logstash/logstash-core/lib/logstash/pipeline/action/create.rb:52:in `execute'", "/opt/cloud/logstash/logstash-core/lib/logstash/agent.rb:388:in `block in converge_state'"]}
19:29:56.151 [LogStash::Runner] INFO logstash.runner - Logstash shut down.
19:29:56.160 [LogStash::Runner] FATAL org.logstash.Logstash - Logstash stopped processing because of an error: (SystemExit) exit
org.jruby.exceptions.SystemExit: (SystemExit) exit
  at org.jruby.RubyKernel.exit(org/jruby/RubyKernel.java:747) ~[jruby-complete-9.2.20.1.jar:7]
  at org.jruby.RubyKernel.exit(org/jruby/RubyKernel.java:710) ~[jruby-complete-9.2.20.1.jar:7]
  at opt.cloud.logstash.lib.bootstrap.environment.<main>(</opt/cloud/logstash/lib/bootstrap/environment.rb:94>) ~[?:?]
Using bundled JDK: /opt/cloud/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/config or /etc/logstash. You can specify the path using --path.settings. Continuing using the defaults
```

4. Run the following command to switch to the directory where the collection channel configuration file is stored:

cd /opt/cloud/logstash/config/files

5. Run the following command to check whether the filter part is abnormal:

cat Configuration file name

If the information shown in the following figure is displayed, the current filter is abnormal.

Figure 12-13 Filter exceptions

```
[root@... ~]# pwd
/opt/cloud/logstash/config/files
[root@... ~]# ll
total 0
-rw-r--r-- 1 root root 1646 Jun 27 19:29 2aac87a8-c8b5-4cc8-8bbb-f74fe1314ca1.conf
drwxr-xr-x 2 root root 4096 Jun 27 19:29 certificate
[root@... ~]# cat 2aac87a8-c8b5-4cc8-8bbb-f74fe1314ca1.conf
input {
  pulsar {
    service_url => "pulsarssl://..."
    is_pw_encrypted => true
    encrypt_key => "..."
    tls_trust_certs_file_path => "/opt/cloud/logstash/config/gemas-pulsar-ca.cert.pem"
    pipes => ["persistent://f690817...
-4638-b445-100000000496"]
    auth_params => {"366639336165623166383435393962303a3a62303665353335303765376436386133363564313338376665643431383838343a3e
633839
3764353
6432653
3338633
3862653
336265383566396164373136653039313530383064373639353334663930326266316331616139346463336435373735393935363939346131633139
3766393138653831323764353566366365"}
    consumer_name => "isap-collector"
    subscription_name => "isap-colle... f74fe1314ca1"
    c8-8bbb-f74fe1314ca1"
  }
}

filter {
  else if [asdfsadsaf] {
    mutate {
      convert => {
        "sadfdd" => "asdfsadf"
      }
    }
  }
}

output {
  file {
    path => "/opt/cloud/logstash/config/a.txt"
    create_if_deleted => true
    codec => "json_lines"
  }
}
```

Solution

- Step 1** Log in to the SecMaster console and access the target workspace.
- Step 2** In the navigation pane on the left, choose **Settings > Collections**. Then, select the **Parsers** tab.
- Step 3** Click **Edit** in the **Operation** column of the row containing the target parser. On the edit page, delete the incorrect configuration and configure it again.

Figure 12-14 Configurations of an abnormal parser

Basic Information

* Name: error_parser

Description: Enter a description. (0/256)

Rules

* Conditional control: Else if

asdfsadf Exist

* Parsing rule: Mutate filter

Convert: sadffd asdfsadf Remove

+ Add

+ Add Configuration

+ Add

Figure 12-15 Modifying the parser configuration

Basic Information

* Name: error_parser

Description: Enter a description. (0/256)

Rules

* Parsing rule: UUID

* Target: uuid

* Overwrite: Yes No

+ Add

Step 4 Click **OK**.

Step 5 Click the **Collection Channels** tab, locate the target connection channel, and click **Restart** in the **Operation** column.

Step 6 Check the status of the collection channel and collection node.

- After the restart is complete, go to the **Collection Channels** tab and check the health status of the target collection channel.
- Select the **Collection Nodes** tab. On the page displayed, check the health status of the target collection node.

If the **Health Status** of the collection channel and collection node is **Normal**, the fault has been rectified.

----End

12.2.3 Common Commands for the Component Controller

Here are some commands you may need to troubleshoot the installation failure of the component controller isap-agent.

- Restart

sh /opt/cloud/isap-agent/action/agent_controller_linux.sh restart

Note: This command will stop and then restart the isap-agent process. You can use command to restart isap-agent if isap-agent fails start or the process does not exist due to a node fault.

- Start

sh /opt/cloud/isap-agent/action/agent_controller_linux.sh start

Note: You can use this command to start isap-agent if isap-agent breaks down but the automatic startup time for disaster recovery does not arrive.

- Stop

sh /opt/cloud/isap-agent/action/agent_controller_linux.sh stop

You can use this command to stop isap-agent. This command will clear the scheduled automatic startup check settings to stop the isap-agent process.

- Checking processes

ps -ef|grep isap-agent

You can use this command to check whether isap-agent is installed on the current host.

- Checking logs

tail -100f /opt/cloud/isap-agent/log/run.log

You can use this command to query the latest 100 lines of logs of the isap-agent service to locate exceptions.

- Disk partitions

sh /opt/cloud/isap-agent/action/agent_controller_linux.sh partition

When you install the collector on a node, you can use this command to partition disks you attach to the node.

A Change History

Released On	Description
2024-10-30	<p>This issue is the third official release.</p> <ul style="list-style-type: none"> • Updated topic "Baseline Inspection": The baseline check function has been fully upgraded. Custom check items and compliance packs are supported. • Updated topic "Adding and Editing an Emergency Policy": Updated operation permissions and limitations and constraints on policies. • Updated the playbook and workflow description in topic "Security Orchestration Overview." • Updated topic "Asset Security Screen": Updated the description of security metrics. • Updated topic "Adding an Asset Connection": Added the concept and function descriptions of asset connections. • Optimized the data collection content and added the operation procedure.

Released On	Description
2024-06-30	<p>This issue is the second official release.</p> <ul style="list-style-type: none"> • Updated topics "Viewing Resource Information" and "Editing and Deleting Resources": Added descriptions about batch edit and optimized some descriptions. • Updated topic "Viewing Baseline Inspection Results": Added the description of the check result page. • Updated topic "Handling Baseline Inspection Results": Added the operation guide to importing and exporting check results. • Updated topics "Viewing Resource Information", "Viewing Vulnerability Details", "Viewing Incidents", "Viewing Alerts", and "Adding and Editing an Indicator": Updated some screenshots. • Added section "Policy Management" to support unified management of emergency policies. • Added some new built-in playbooks and workflows in "Built-in Playbooks and Workflows." • Added topic "Managing Workspace Tags." • Added topic "One-Click Blocking or Unblocking." • Updated the playbook and workflow description in topic "Security Orchestration Overview."
2024-02-23	<p>This issue is the first official release.</p>